

DIGITAL INFRASTRUCTURE FOR E-GOVERNANCE IN UGANDA
-
**A CASE STUDY OF THE MINISTRY OF FINANCE, PLANNING AND ECONOMIC
DEVELOPMENT (MOFPED)**

Research Article on

Digital Infrastructure for E-Governance in Uganda: Cloud, Intranets, and Foundational ICTs at
the Ministry of Finance, Planning and Economic Development (MOFPED)

Author

George Hillary Kafuko

Registration Number: **2500726384** | Student Number: **2025/HD05/26384U**

Institution / Department: Makerere University / College of Computing and Information
Sciences

Programme: Master of E-Governance Technology and Services

Course: METS 7106 - Practical Skills for E-Governance and Technical Services

Supervisor: Dr. Annabella Habinka Ejiri

Date of Submission: 19 December 2025

ABSTRACT

Digital infrastructure forms the backbone of effective e-governance by enabling secure, reliable, and scalable delivery of public services. In Uganda, Ministries, Departments, and Agencies (MDAs) increasingly depend on foundational ICT systems such as government intranets, data centres, and hybrid hosting environments to support digital financial management and inter-agency collaboration. This article examines the role of digital infrastructure in advancing e-governance, using the Ministry of Finance, Planning and Economic Development (MOFPED) as a case study based on an apprenticeship placement within the Ministry's Management Information Systems (MIS) Department.

The study seeks to understand how core infrastructure components including networking, hosting platforms, security controls, and service management tools collectively support digital service delivery and institutional efficiency at MOFPED. A qualitative case study approach was adopted, drawing on structured interviews with technical team leads, direct observation during the apprenticeship period, and analysis of internal operational practices. Data was thematically analysed to assess infrastructure design choices, operational challenges, and governance implications.

Key findings indicate that MOFPED has made significant progress in establishing resilient on-premise infrastructure supported by virtualization, secure intranets, and centralized identity management. However, constraints such as legacy systems, limited cloud adoption, connectivity bottlenecks in remote sites, and stringent security controls continue to shape infrastructure decisions. The study highlights the trade-offs between control, security, scalability, and service accessibility within a high-sensitivity government environment.

The article contributes practical insights into how foundational ICT infrastructure enables e-governance in resource-constrained public institutions and offers recommendations for phased cloud integration, improved inter-MDA connectivity, and infrastructure-driven citizen-centric service delivery.

Keywords: e-governance, digital infrastructure, government ICT, intranet systems, cloud computing, MOFPED, Uganda

1. INTRODUCTION

1.1 Background and Context of E-Governance

E-Governance broadly refers to the application of information and communication technologies (ICTs) to enhance the delivery of government services, improve internal efficiency, strengthen transparency, and promote citizen participation in public administration. Internationally, institutions such as the United Nations and the World Bank conceptualize e-governance as more than mere digitization of services. It is viewed as a transformational approach that reshapes how governments interact with citizens, businesses, and other state institutions. The United Nations defines e-governance as the use of ICTs to improve the access to and delivery of government services, strengthen democratic processes, and enhance public sector accountability, while the World Bank emphasizes its role in improving governance outcomes through efficiency, effectiveness, and inclusiveness.

In developing country contexts such as Uganda, e-governance has emerged as a strategic response to long-standing public sector challenges, including bureaucratic inefficiencies, fragmented service delivery, limited inter-agency coordination, and constrained fiscal resources. The Government of Uganda has, over the past two decades, increasingly adopted ICT-enabled reforms to modernize public administration, with a particular focus on financial management, procurement transparency, and service standardization across Ministries, Departments, and Agencies (MDAs). These reforms have been guided by national frameworks such as the National ICT Policy and the e-Government Strategy, implemented under the coordination of the National Information Technology Authority-Uganda (NITA-U).

Within this national landscape, digital infrastructure serves as the foundational layer upon which all e-governance initiatives are built. Unlike visible front-end systems such as portals or mobile applications, infrastructure components including networks, data centres, hosting platforms, intranets, and security mechanisms operate largely in the background. However, their reliability, scalability, and security directly determine the success or failure of digital public services. Weak infrastructure can undermine even the most well-designed digital systems, while robust infrastructure enables continuity, trust, and institutional resilience.

1.2 Evolution of ICT Use in Government Operations

The evolution of ICT use in government has followed a gradual trajectory from basic computerization to integrated digital ecosystems. Early ICT adoption in the Ugandan public sector focused primarily on automating isolated administrative functions such as payroll processing, document preparation, and basic record keeping. These systems were often standalone, department-specific, and heavily dependent on manual intervention, resulting in limited efficiency gains and persistent data silos.

Over time, the focus shifted toward integrated information systems designed to support core government functions. At MOFPED, this transition is evident in the implementation of large-scale systems such as the Integrated Financial Management System (IFMS), Program Budgeting System (PBS), and Electronic Government Procurement (e-GP). These platforms marked a significant shift toward centralized data management, standardized workflows, and real-time financial oversight. However, their effectiveness has been closely tied to the availability of stable networks, secure hosting environments, and reliable intranet connectivity across central and local government entities.

More recently, global trends toward cloud computing, virtualization, and shared services have influenced government ICT strategies. In Uganda, this evolution has been moderated by

considerations of data sovereignty, security sensitivity, and institutional capacity. As a result, many MDAs, including MOFPED, have adopted hybrid infrastructure models that combine on-premise data centres with externally hosted services managed by NITA-U. This approach reflects a cautious but deliberate effort to balance control, compliance, and scalability within a high-risk financial governance environment.

1.3 Importance of Digital Infrastructure in Public Sector E-Governance

Digital infrastructure plays a critical enabling role in public sector governance, particularly in institutions responsible for national financial oversight. At MOFPED, infrastructure underpins virtually all core operations, ranging from budget formulation and execution to inter-ministerial reporting and donor coordination. Secure intranets facilitate internal communication and system access, while wide area networks (WANs) enable connectivity between headquarters, regional offices, and other MDAs.

The sensitivity of financial and economic data handled by MOFPED imposes stringent requirements on infrastructure design. Systems must guarantee confidentiality, integrity, and availability, while also supporting high transaction volumes and inter-system interoperability. Infrastructure decisions therefore extend beyond technical considerations to encompass governance issues such as access control, separation of duties, auditability, and compliance with national information security standards.

Furthermore, digital infrastructure directly influences service delivery outcomes beyond the Ministry itself. Systems hosted and managed at MOFPED, such as IFMS and PBS, serve as backbone platforms for other government entities. Any infrastructure disruption can have cascading effects across the public sector, affecting service delivery to citizens, suppliers, and development partners. This interconnectedness underscores the strategic importance of investing in resilient and well-governed ICT foundations.

1.4 Research Gap and Focus of the Study

While substantial literature exists on e-governance strategies, digital service delivery, and citizen-facing platforms, comparatively less attention has been paid to the operational realities of digital infrastructure within government institutions in developing countries. Existing studies often emphasize policy frameworks and user adoption, while treating infrastructure as a static or secondary component. In practice, however, infrastructure constraints frequently shape what is feasible in terms of service design, system integration, and scalability.

This study addresses this gap by focusing explicitly on digital infrastructure as an enabler and constraint of e-governance within a critical government institution. Drawing on direct apprenticeship experience at MOFPED, the article examines how cloud considerations, intranet architectures, hosting strategies, and foundational ICT controls are implemented, governed, and experienced in day-to-day operations. The emphasis is on practical insights rather than abstract models, grounded in the realities of a high-stakes financial governance environment.

1.5 Research Objectives

Guided by the above context, this article is structured around the following objectives:

1. To examine the role of digital infrastructure in supporting e-governance operations at the Ministry of Finance, Planning and Economic Development.
2. To analyse the design, management, and governance of core infrastructure components, including networks, hosting platforms, and security controls.

3. To identify key challenges and trade-offs influencing infrastructure decisions in a public sector financial institution and propose lessons applicable to other MDAs.

2. LITERATURE REVIEW: E-GOVERNANCE STRATEGY AND IMPLEMENTATION

2.1 E-Governance Strategy as an Enabler of Public Sector Transformation

E-governance strategy is commonly understood as the structured use of digital technologies to support public sector objectives through improved efficiency, transparency, and accountability. However, contemporary literature increasingly frames e-governance strategy not as a technology agenda, but as an institutional transformation process that reshapes how governments organize work, manage information, and interact with stakeholders. In this view, digital systems are tools through which broader governance goals are pursued, rather than ends in themselves. In other words, digital systems are implemented to support good governance, such as accountability, efficiency, and transparency, rather than existing as objectives by themselves.

International development institutions such as the World Bank argue that effective e-governance strategies must be embedded within existing public sector reform efforts, particularly in areas such as public financial management, service standardization, and performance monitoring. The United Nations further emphasizes that e-governance should enhance inclusiveness and trust in government, requiring strategies that are citizen-oriented, secure, and sustainable. These perspectives converge on a critical point: without a coherent strategy linking technology investments to institutional mandates, digital initiatives risk becoming fragmented, underutilized, or unsustainable.

In practice, strategy formulation in e-governance is shaped by a country's administrative maturity, regulatory environment, and fiscal capacity. In developing countries, strategies often emerge incrementally, driven by donor-funded projects or sector-specific reforms rather than a single, unified digital vision. This has implications for infrastructure planning, as systems are frequently deployed to meet immediate operational needs without sufficient consideration of long-term scalability or interoperability.

2.2 Digital Infrastructure in E-Governance Literature

Digital infrastructure occupies a central but often understated position in e-governance scholarship. While much of the literature focuses on online service delivery, portals, and user engagement, foundational infrastructure such as networks, data centres, hosting platforms, and intranets receive comparatively less analytical attention. Yet, multiple studies acknowledge that infrastructure quality is a decisive factor in determining the reliability and credibility of digital government systems.

Scholars examining e-governance in low and middle-income countries consistently identify infrastructure limitations as a primary constraint. These include unreliable connectivity, limited redundancy, outdated hardware, and insufficient disaster recovery mechanisms. In response, governments have pursued different infrastructure models, ranging from fully centralized government data centres to decentralized, agency-owned systems and, more recently, hybrid and cloud-based architectures.

The literature suggests that no single model is universally optimal. Centralized infrastructure can promote standardization and cost efficiency, but it may introduce systemic risks and reduce institutional flexibility. Decentralized models allow agencies greater control over sensitive systems but often result in duplication and higher operational costs. Hybrid approaches attempt

to balance these trade-offs by centralizing shared services while allowing mission-critical systems to remain under agency control.

2.3 E-Governance Strategy and Infrastructure in Sub-Saharan Africa

Empirical studies from Sub-Saharan Africa highlight the complex relationship between e-governance ambitions and infrastructure realities. Governments in the region have made notable investments in national backbone networks and data centres, often supported by development partners. These investments have enabled progress in areas such as financial management systems, tax administration, and procurement transparency.

However, the literature also documents persistent challenges. Infrastructure rollouts frequently outpace institutional readiness, resulting in systems that are technically functional but poorly integrated into organizational workflows. Additionally, uneven connectivity between urban and rural areas limits the effectiveness of centralized systems, particularly for MDAs with decentralized operations.

Another recurring theme is the tension between modernization and risk management. Public institutions handling sensitive financial, security, or personal data tend to adopt conservative infrastructure strategies, prioritizing control and compliance over innovation. This risk-averse posture can slow the adoption of cloud services and shared platforms, even where potential efficiency gains are evident.

2.4 Uganda's E-Governance and Institutional Coordination

Uganda's e-governance strategy is anchored in national ICT policies that promote digital transformation as a driver of public sector efficiency and economic development. The establishment of the National Information Technology Authority-Uganda (NITA-U) marked a significant step toward centralizing ICT coordination, standard-setting, and shared infrastructure provision across government.

Literature on Uganda's e-governance implementation recognizes the progress made in developing the National Backbone Infrastructure and government data centre services. These initiatives have improved inter-MDA connectivity and supported the rollout of key national systems. At the same time, scholars note that institutional coordination remains uneven, with variations in ICT capacity, governance maturity, and risk tolerance across MDAs.

For institutions such as the Ministry of Finance, Planning and Economic Development, infrastructure decisions are shaped by additional layers of accountability. As the custodian of national financial systems, MOFPED operates under heightened scrutiny from auditors, development partners, and oversight bodies. This context influences the Ministry's cautious approach to outsourcing and cloud adoption, as reflected in literature emphasizing the importance of data sovereignty and internal control in public financial management systems.

2.5 Legal, Ethical, and Social Dimensions of Infrastructure Strategy

Legal and regulatory frameworks play a critical role in shaping e-governance infrastructure choices. Data protection legislation, public finance regulations, and information security standards impose obligations on public institutions regarding how data is stored, accessed, and shared. The literature emphasizes that non-compliance can expose governments to legal liability, reputational damage, and loss of public trust.

Ethical considerations further complicate infrastructure strategy. Centralized systems can improve oversight and reduce corruption, but they also raise concerns about surveillance, misuse

of data, and exclusion of digitally marginalized groups. Scholars argue that ethical e-governance requires infrastructure designs that protect user privacy while enabling accountability and transparency.

Social and organizational factors are equally influential. Resistance to change, skills gaps, and weak ownership structures can undermine infrastructure investments. Studies consistently show that infrastructure effectiveness depends not only on technical robustness but also on user confidence, institutional incentives, and leadership commitment.

2.6 Theoretical Foundations for Understanding Infrastructure Adoption

Several theoretical perspectives help explain how digital infrastructure is adopted and used within government institutions. The Technology Acceptance Model (TAM) highlights the role of perceived usefulness and reliability in shaping user engagement with digital systems. In infrastructure-heavy environments, reliability and system availability often outweigh usability considerations, particularly for mission-critical applications.

Diffusion of Innovation theory provides insight into how new infrastructure models, such as cloud computing, are spread within the public sector. Adoption tends to be gradual, influenced by risk perceptions, compatibility with existing systems, and the presence of institutional champions. In hierarchical public organizations, diffusion is often driven by policy mandates rather than grassroots experimentation.

Institutional theory further explains why public institutions may retain legacy infrastructure even when more efficient alternatives exist. Formal rules, audit requirements, and established routines create path dependencies that shape technology choices. Understanding these dynamics is essential for analysing infrastructure strategy in high-stakes government environments such as MOFPED.

3. METHODOLOGY

3.1 Research Design

This study adopted a qualitative case study research design, focusing on the Ministry of Finance, Planning and Economic Development (MOFPED) as a single, information-rich case of e-governance implementation in Uganda. A case study approach was considered appropriate due to the study's emphasis on understanding how and why digital infrastructure is designed, governed, and operationalized within a specific institutional context.

Qualitative methods were particularly suitable because the research sought to capture operational realities, decision-making processes, and institutional constraints that are not easily quantifiable. Rather than measuring system performance through numerical indicators alone, the study aimed to explore experiences, practices, and perspectives of technical teams responsible for core ICT infrastructure. This approach aligns with e-governance research that prioritizes contextual depth and institutional understanding over broad generalization.

The case of MOFPED was deliberately selected due to its central role in national financial governance and its reliance on mission-critical digital systems. As the custodian of platforms such as the Integrated Financial Management System and the Program Budgeting System, the Ministry provides a meaningful environment for examining the relationship between digital infrastructure and effective public sector governance.

3.2 Study Context and Population

The study was conducted within the Management Information Systems (MIS) Department at MOFPED, where I (the researcher) undertook an e-governance apprenticeship during the semester. The MIS Department is responsible for planning, implementing, securing, and supporting the Ministry's ICT infrastructure and digital systems.

The study population consisted of technical and managerial staff directly involved in infrastructure-related functions. These included officers from the following units:

- Information Security
- Networking
- Hosting and Data Centre Operations
- Applications Management
- Service Desk and User Support
- Supervisory and Management Roles within the MIS

These units were selected because of their direct involvement in the design, operation, and governance of digital infrastructure that supports both internal Ministry operations and inter-MDA systems.

3.3 Sampling Technique

A purposive sampling technique was employed to identify respondents with relevant knowledge and experience in digital infrastructure management. Participants were selected based on their functional roles, decision-making responsibilities, and direct involvement in ICT operations at MOFPED.

This approach ensured that data was collected from individuals who possessed practical insights into infrastructure planning, system integration, security controls, and operational challenges. Given the specialized nature of the subject matter, random sampling was not considered appropriate, as it could have included participants without sufficient exposure to infrastructure-related processes.

3.4 Data Collection Methods

Multiple qualitative data collection methods were used to enhance the credibility and depth of the study.

Semi-structured interviews were conducted with technical leads and section heads across the MIS Department. These interviews were guided by a structured questionnaire developed specifically for the apprenticeship, covering areas such as security management, hosting strategies, networking architecture, service desk operations, and application support. The semi-structured format allowed for consistency across interviews while providing flexibility to explore emerging issues in greater depth.

Direct observation formed a key component of the methodology. Through day-to-day engagement during the apprenticeship, I observed infrastructure operations, incident handling, system maintenance activities, and inter-team coordination. This method provided first-hand insight into operational workflows and informal practices that are often undocumented.

Additionally, national policy documents and publicly available reports on e-governance and ICT infrastructure in Uganda were examined to situate institutional practices within a broader policy context.

3.5 Data Collection Tools and Instruments

The primary data collection instrument was a structured interview guide in the form of a questionnaire, developed by myself to support consistent engagement with different technical units. The guide covered thematic areas aligned with the study objectives, including infrastructure design, security practices, system integration, and operational challenges.

Basic face-to-face sitdowns and interactions were used to coordinate interviews and document observations. No automated data extraction or advanced analytics tools were employed, as the study focused on qualitative insights rather than large-scale data analysis.

3.6 Data Analysis Techniques

Data analysis was conducted using thematic analysis, a qualitative method suitable for identifying patterns and recurring themes across interview responses and observational notes. Interview data and field notes were reviewed iteratively, with key themes coded around infrastructure governance, operational efficiency, risk management, and institutional constraints. Themes were then compared across functional units to identify areas of convergence and divergence. This process enabled the study to develop a holistic understanding of how different infrastructure components interact to support e-governance at MOFPED.

3.7 Project Management Perspective

Given that infrastructure initiatives at MOFPED are typically implemented as structured projects, the study also adopted a project management lens in its analysis. While no single formal framework was explicitly imposed, practices observed during the apprenticeship reflected principles from established methodologies such as PMBOK, including defined scopes, change management processes, risk assessment, and stakeholder coordination.

This perspective was useful in analysing how infrastructure upgrades, system deployments, and maintenance activities are planned and executed within a regulated public sector environment. It also provided a basis for linking infrastructure management practices to broader e-governance outcomes.

3.8 Ethical Considerations

Ethical considerations were observed throughout the study. Participation in interviews was voluntary, and respondents were informed of the academic purpose of the research. Sensitive operational details were treated with confidentiality, and findings are presented at an aggregate level to avoid exposing specific vulnerabilities.

I adhered to institutional guidelines governing apprenticeship conduct and research ethics, ensuring that observations and data collection did not interfere with normal operations or compromise information security.

4. SYSTEM / PROJECT DESIGN: GOVERNMENT DIGITAL INFRASTRUCTURE AT MOFPED

4.1 Overview of the Digital Infrastructure Architecture

The digital infrastructure at the Ministry of Finance, Planning and Economic Development (MOFPED) is designed to support high-availability, security-sensitive, and transaction-intensive government systems. Rather than operating as a single monolithic platform, the infrastructure is composed of interconnected layers that collectively enable internal operations, inter-ministerial coordination, and national financial service delivery.

At a high level, the infrastructure architecture comprises four primary layers: network connectivity, hosting and compute resources, application platforms, and security and access control mechanisms. These layers are tightly integrated to ensure continuity, data integrity, and controlled access across the Ministry's systems. The architecture reflects a deliberate design choice that prioritizes reliability and control over rapid experimentation, consistent with MOFPED's mandate as the custodian of public financial systems.

Most core systems are hosted within internally managed data centre environments, supported by virtualization technologies that allow efficient resource allocation and redundancy. External hosting is selectively adopted, mainly through government-coordinated platforms provided by NITA-U, where systems benefit from shared infrastructure while remaining subject to national oversight and standards.

4.2 Network and Intranet Design

MOFPED's intranet forms the backbone of internal digital operations, enabling secure communication and system access across departments. The intranet is supported by a wide area network that connects the Ministry's headquarters to other government entities and regional offices through links provided by NITA-U and selected telecommunications partners.

The network design emphasizes segmentation and controlled access. Virtual Local Area Networks (VLANs) and firewall rules are used to separate user groups, applications, and system environments. This approach minimizes lateral movement within the network and reduces the potential impact of security incidents. Access to sensitive systems is restricted based on role, function, and approval level, reinforcing the principle of least privilege.

Monitoring tools are employed to track network performance, availability, and potential bottlenecks. Visual dashboards and alert mechanisms enable the technical teams to respond proactively to incidents such as congestion, hardware failures, or link degradation. While the core network infrastructure has matured over time, challenges remain, particularly in relation to dependency on external service providers and aging equipment in some connectivity segments.

4.3 Hosting, Compute, and Storage Design

Hosting at MOFPED is primarily centered on on-premise infrastructure supported by virtualization technologies. The use of virtual machines allows multiple systems to run on shared physical hardware while maintaining isolation and flexibility. This design supports high availability by enabling rapid failover, resource reallocation, and parallel system instances for critical applications.

Storage architecture combines disk-based systems for active data with archival mechanisms for long-term retention and backup. Regular backups are conducted, with replication to recovery sites for mission-critical systems. This layered approach to data protection aligns with the Ministry's emphasis on business continuity and disaster recovery, particularly given the national impact of system outages in financial governance platforms.

While cloud computing features prominently in global e-governance discourse, MOFPED's adoption has been cautious and selective. Concerns related to data sovereignty, regulatory compliance, and auditability influence hosting decisions, especially for systems that process budgetary, procurement, and payment data. As a result, cloud considerations at MOFPED are evaluated less as a cost-saving measure and more as a governance and risk management issue.

4.4 Application Environment and Interoperability Design

The infrastructure is designed to support a diverse portfolio of applications, including the Integrated Financial Management System, Program Budgeting System, Electronic Government Procurement platform, and other supporting tools. These systems are developed and maintained through a combination of vendor-supported solutions and internally managed applications.

Interoperability is achieved through standardized interfaces and shared identifiers that enable data exchange between systems and across MDAs. Application integration is governed by formal agreements and change management processes to ensure consistency and security. This structured approach reduces the risk of data inconsistency and supports coordinated decision-making across government.

However, interoperability remains constrained by legacy systems and uneven connectivity in some government entities. In such cases, manual workarounds and offline processes are occasionally employed to maintain continuity, highlighting the dependence of application performance on underlying infrastructure quality.

4.5 Security-by-Design Principles

Security is embedded into infrastructure design rather than treated as an add-on. MOFPED employs a zero-trust philosophy that assumes no implicit trust within the network. Authentication, authorization, and access controls are enforced at multiple layers, supported by centralized identity management systems.

Data protection mechanisms address both data in transit and data at rest. Secure network tunnels, encryption, and controlled access policies are used to protect sensitive information. System patching, license management, and vulnerability monitoring are handled through structured processes aligned with national security guidelines.

Notably, design decisions often favor security over convenience. Remote access to internal systems is tightly restricted, and flexibility such as remote working is limited due to the sensitivity of financial data. While this approach can affect user experience, it reflects a conscious trade-off aligned with MOFPED's risk profile.

4.6 Usability and Internal User Experience Considerations

Although citizen-facing usability is a major focus in many e-governance initiatives, infrastructure design at MOFPED primarily targets internal users such as accountants, planners, auditors, and system administrators. User experience considerations therefore focus on reliability, predictability, and clarity of system access rather than visual design.

Access to systems is standardized through intranet-based entry points and controlled authentication mechanisms. Training, documentation, and service desk support play a significant role in enabling effective use of infrastructure-supported systems. Where usability challenges arise, they are often linked to connectivity limitations or system complexity rather than interface design alone.

4.7 Infrastructure Design Trade-offs and Constraints

The literature emphasizes that infrastructure design in the public sector involves continuous trade-offs, and MOFPED provides a clear illustration of this reality. Decisions around centralization, cloud adoption, and access flexibility are shaped by competing priorities such as, security versus accessibility, control versus scalability, and innovation versus compliance.

Budgetary constraints, dependency on external providers, and legacy system compatibility further influence design choices. These constraints do not indicate a lack of strategic intent but

rather reflect the operational realities of managing national financial systems in a developing country context like Uganda's.

5. FINDINGS AND RESULTS: DIGITAL SERVICE DELIVERY, DATA SECURITY, AND INFRASTRUCTURE ANALYTICS

5.1 Overview of Findings

This section presents the key findings from the apprenticeship-based case study at the Ministry of Finance, Planning and Economic Development (MOFPED). Findings are drawn from interviews with technical teams, direct observation, and review of operational practices within the Management Information Systems Department. The results are organized around three interrelated dimensions, and these are: digital service delivery effectiveness, data security and risk management, and the use of infrastructure-related information for operational decision-making.

Overall, the findings indicate that MOFPED's digital infrastructure plays a central enabling role in public financial governance. At the same time, infrastructure-related constraints significantly influence how services are delivered, secured, and scaled across government.

5.2 Digital Service Delivery Supported by Infrastructure

MOFPED supports several mission-critical digital services that underpin government financial operations. Systems such as the Integrated Financial Management System, Program Budgeting System, and Electronic Government Procurement platform rely heavily on stable infrastructure to function effectively across central government and affiliated MDAs.

Findings show that infrastructure reliability directly affects service continuity. Internally hosted systems benefit from high availability mechanisms enabled through virtualization and redundancy. For critical applications, multiple system instances are maintained to minimize downtime and ensure continuity during maintenance or failure scenarios. Scheduled upgrades and patching are conducted during controlled time windows, reducing disruption to daily operations.

However, service delivery effectiveness varies depending on connectivity conditions at user locations. While headquarters and well-connected MDAs experience relatively stable access, remote sites face intermittent connectivity challenges. In such cases, users resort to manual processes or delayed system interactions, which can undermine the efficiency gains intended by digital service deployment.

From a service management perspective, the internal service desk plays a coordinating role in incident resolution. Issues are classified based on severity and routed to relevant technical teams. The presence of service-level expectations and a knowledge base has improved response consistency, although the volume of user requests and digital skills gaps continue to strain support capacity.

5.3 Infrastructure-Enabled Efficiency Gains

One of the notable findings relates to how infrastructure has contributed to efficiency improvements in financial operations. Centralized systems have reduced duplication of data entry, improved real-time visibility of financial transactions, and strengthened audit trails. Compared to earlier manual or semi-automated processes, digital systems supported by secure infrastructure allow faster consolidation of financial information and improved coordination between departments.

Infrastructure standardization has also simplified system administration. Virtualization enables faster provisioning of resources, while centralized monitoring tools support proactive issue detection. These efficiencies are particularly important in an environment where infrastructure downtime can have national-level implications.

Despite these gains, the findings also highlight diminishing returns when infrastructure expansion is constrained by legacy systems. Newer applications often require greater computing resources and compatibility adjustments, increasing operational costs and complexity.

5.4 Data Security and Risk Management Outcomes

Data security emerged as a dominant consideration shaping infrastructure outcomes at MOFPED. Findings indicate a strong institutional emphasis on protecting both data in transit and data at rest. Network-level security controls, secure tunnels, and access segmentation are employed to safeguard data flows between systems and users.

At the system level, centralized identity and access management ensures that users can only access resources aligned with their roles. Separation of duties is strictly enforced, particularly for high-privilege accounts. This approach reduces insider risk and supports compliance with audit and regulatory requirements.

The security team operates within a structured governance framework that includes escalation matrices, incident classification, and regular updates informed by national security advisories. Notably, convenience is intentionally deprioritized in favor of security. Remote access to internal systems is heavily restricted, and flexibility such as remote working has been curtailed following heightened risk assessments.

Challenges persist in managing human-related security risks, particularly social engineering and user behavior. Additionally, storage constraints have necessitated difficult decisions around data retention and archival, balancing operational needs against infrastructure capacity.

5.5 Use of Infrastructure Information for Operational Decision-Making

While advanced data analytics is often highlighted in e-governance literature, findings from MOFPED indicate a more pragmatic use of infrastructure-related data. Monitoring tools provide real-time visibility into system performance, resource utilization, and network health. This information supports operational decisions such as capacity planning, maintenance scheduling, and incident prioritization.

Dashboards and alerts enable teams to identify trends such as recurring network bottlenecks or resource saturation. However, from my observation, the use of predictive analytics or advanced data-driven optimization remains limited. Decisions are primarily reactive or incremental, informed by operational experience rather than formal analytics models.

This finding reflects a broader reality in many public sector environments, where the primary value of infrastructure data lies in maintaining stability and compliance rather than driving innovation. Nevertheless, the existing monitoring practices provide a foundation upon which more advanced analytics capabilities could be developed in the future.

5.6 Summary of Key Findings

In summary, the findings demonstrate that:

- Digital service delivery at MOFPED is highly dependent on the reliability and governance of underlying infrastructure.

- Infrastructure investments have delivered tangible efficiency gains but are moderated by connectivity gaps and legacy system constraints.
- Security considerations dominate infrastructure design and operation, often at the expense of flexibility and user convenience.
- Infrastructure-related data is actively used for operational monitoring but not yet fully leveraged for strategic analytics or optimization.

These findings provide the empirical basis for the discussion in the next section, where infrastructure outcomes are interpreted in relation to citizen engagement, institutional collaboration, and broader e-governance objectives.

6. DISCUSSION: DIGITAL INFRASTRUCTURE, CITIZEN ENGAGEMENT, AND GOVERNANCE OUTCOMES

6.1 Digital Infrastructure as an Enabler of Institutional Effectiveness

The findings from MOFPED confirm the central argument in e-governance literature that digital infrastructure is not a peripheral technical concern but a core determinant of institutional effectiveness. The Ministry's ability to deliver reliable financial services, maintain data integrity, and coordinate with other MDAs is fundamentally anchored in the stability and governance of its underlying ICT infrastructure.

The observed emphasis on internally controlled hosting, secure intranet access, and redundancy aligns with theoretical perspectives that position infrastructure as a strategic asset in high-risk public sector environments. In institutions where system failure can disrupt national financial operations, infrastructure design decisions prioritize predictability and control over rapid innovation. This reinforces the view that e-governance maturity should be assessed not only by the number of digital services offered, but by the resilience of the systems that support them.

6.2 Infrastructure and Citizen-Centric Service Delivery

Although MOFPED is not a direct citizen service provider in the traditional sense, its infrastructure decisions have downstream implications for citizen-facing services across government. Systems such as IFMS and e-GP indirectly shape citizen experiences by influencing procurement efficiency, payment timelines, and public expenditure transparency.

The findings suggest that infrastructure reliability contributes to improved service predictability, which in turn affects public trust. Conversely, connectivity limitations and system downtimes at peripheral MDAs can delay service delivery to citizens, even when central systems are functioning effectively. This highlights an often-overlooked dimension of citizen-centric e-governance which is, the dependence of front-end service quality on back-end infrastructure conditions across the entire government ecosystem.

From an inclusion perspective, infrastructure disparities between central and remote offices reinforce digital divides within government itself. These internal divides can translate into unequal service outcomes for citizens, underscoring the need for infrastructure strategies that explicitly address geographic and institutional equity.

6.3 Security, Trust, and Governance Trade-offs

The strong security posture observed at MOFPED reflects a governance environment characterized by high accountability and low tolerance for risk. The adoption of zero-trust principles, strict access controls, and limited remote access demonstrates an institutional prioritization of data protection and audit compliance.

While such measures enhance system integrity and reduce exposure to cyber threats, they also introduce trade-offs related to usability and operational flexibility. The literature acknowledges this tension, noting that excessive security constraints can hinder productivity and slow innovation if not carefully balanced. At MOFPED, these trade-offs appear to be consciously accepted, reflecting the Ministry's assessment that the cost of security breaches outweighs the benefits of convenience.

This finding reinforces the argument that e-governance strategies must be context-sensitive. What may be considered overly restrictive in a service-oriented agency may be entirely appropriate in a financial governance institution with national-level risk exposure.

6.4 Infrastructure Governance and Inter-Agency Coordination

This discussion also reveals the importance of infrastructure governance in enabling or constraining inter-agency collaboration. MOFPED's reliance on shared connectivity and externally provided services through NITA-U illustrates the benefits of centralized coordination, including standardization and cost-sharing.

However, the findings suggest that coordination challenges persist, particularly where infrastructure dependencies intersect with institutional autonomy. Differences in ICT maturity, resource availability, and risk tolerance across MDAs complicate efforts to achieve seamless interoperability. These challenges align with regional studies that caution against assuming uniform readiness across government entities.

Effective infrastructure governance therefore requires not only technical standards but also clear roles, accountability mechanisms, and sustained capacity building across MDAs. Without these, shared infrastructure risks becoming a bottleneck rather than an enabler of e-governance.

6.5 Infrastructure Data and the Limits of Analytics in Practice

While the literature increasingly emphasizes data analytics as a driver of evidence-based governance, the MOFPED case highlights a more constrained reality. Infrastructure-related data is primarily used for operational monitoring and incident management rather than strategic analytics or predictive decision-making.

This does not indicate a failure of e-governance, but rather reflects pragmatic prioritization. In a resource-constrained and risk-sensitive environment, maintaining system stability takes precedence over exploratory analytics. Nonetheless, the existence of monitoring tools and structured data collection provides a foundation upon which more advanced analytics capabilities could be incrementally developed.

This finding contributes to the literature by illustrating the staged nature of analytics adoption in government, where foundational stability is a prerequisite for higher-level data-driven innovation.

6.6 Contribution to E-Governance Knowledge and Practice

By grounding analysis in apprenticeship-based evidence, this study contributes a practitioner-informed perspective to e-governance scholarship. It demonstrates how digital infrastructure decisions are shaped by institutional mandates, risk considerations, and operational constraints, rather than abstract policy ideals.

The MOFPED case reinforces the argument that successful e-governance depends as much on infrastructure governance and organizational context as on technology selection. These insights

are particularly relevant for developing countries seeking to scale digital government initiatives while managing fiscal and security risks.

7. CONCLUSION AND RECOMMENDATIONS: FUTURE DIRECTIONS FOR E-GOVERNANCE

7.1 Conclusion

This study examined the role of digital infrastructure in enabling e-governance within the Ministry of Finance, Planning and Economic Development, focusing on cloud considerations, intranet systems, and foundational ICTs. Drawing on an apprenticeship-based case study, the research demonstrated that infrastructure is not merely a technical foundation but a strategic enabler of public financial governance.

The findings show that MOFPED has established a relatively mature infrastructure environment characterized by internal hosting, secure intranet connectivity, and structured service management. These elements support the reliability, integrity, and accountability required of national financial systems. At the same time, the study revealed persistent constraints, including legacy system dependencies, uneven connectivity across MDAs, limited adoption of cloud-based services, and trade-offs between security and operational flexibility.

Importantly, the research highlights that e-governance success in high-risk institutions cannot be evaluated solely by service digitization metrics. Instead, success must be understood in terms of infrastructure resilience, governance discipline, and the institution's ability to manage risk while sustaining service continuity. MOFPED's experience illustrates how cautious, control-oriented infrastructure strategies can be appropriate and effective within sensitive public sector environments.

7.2 Implications for E-Governance Policy and Practice

The case of MOFPED underscores several broader implications for e-governance implementation in Uganda and similar contexts. First, national e-governance strategies must recognize infrastructure as a long-term public investment rather than a one-off technical project. Sustainable digital government requires continuous funding, skills development, and governance refinement.

Second, centralized coordination through entities such as NITA-U offers clear benefits in terms of standardization and shared services, but must be complemented by institution-specific flexibility for agencies with specialized mandates. A one-size-fits-all infrastructure model is unlikely to accommodate the diverse risk profiles and operational needs of all MDAs.

Finally, the study demonstrates the value of embedding practical learning mechanisms, such as apprenticeships, within e-governance programs. Such approaches bridge the gap between policy intent and operational reality, contributing to more grounded and implementable digital governance strategies.

7.3 Future Trends in E-Governance Infrastructure

Looking ahead, several trends are likely to shape the evolution of e-governance infrastructure in Uganda. Cloud computing will continue to feature in policy discussions, particularly as a means of improving scalability and cost efficiency. However, adoption in sensitive institutions is likely to remain gradual and selective, focusing on non-core systems or hybrid models that preserve data sovereignty.

Advances in cybersecurity tools, including automated threat detection and centralized security monitoring, may strengthen the protection of government systems. Similarly, improvements in national connectivity infrastructure could reduce disparities between central and remote offices, enhancing consistency in service delivery.

Emerging technologies such as artificial intelligence and advanced analytics have potential applications in areas such as fraud detection, expenditure analysis, and performance monitoring. However, their effective use will depend on the stability and quality of underlying infrastructure, reinforcing the importance of foundational ICT investment.

7.4 Recommendations

Based on the findings and analysis, the following recommendations are proposed:

1. **Adopt a phased hybrid cloud strategy:** MOFPED and similar institutions should explore limited cloud adoption for non-sensitive systems, supported by clear governance frameworks and risk assessments, while retaining internal control over core financial platforms.
2. **Strengthen inter-MDA connectivity and redundancy:** Continued investment in network reliability, particularly for remote and decentralized offices, is essential to ensure consistent system access and reduce reliance on manual workarounds.
3. **Enhance infrastructure capacity planning:** Regular assessment of compute, storage, and network capacity should be institutionalized to anticipate growth in system demands and avoid reactive upgrades.
4. **Invest in security awareness and user capability:** Technical controls should be complemented by ongoing user education to mitigate human-related security risks such as social engineering and poor access practices.
5. **Leverage infrastructure monitoring data strategically:** Existing monitoring tools should be gradually extended beyond operational use to inform strategic planning, resource allocation, and system modernization decisions.
6. **Formalize and enforce a tiered ICT support model:** MOFPED should implement a clearly defined Level 1, Level 2, and Level 3 support structure that empowers regional and on-ground ICT staff to resolve routine issues locally, enforces structured escalation protocols, and reduces unnecessary centralization of support services at headquarters.

7.5 Closing Remarks

In conclusion, this study affirms that digital infrastructure is a decisive factor in the success of e-governance initiatives. The MOFPED case provides practical lessons on balancing innovation, control, and sustainability in a developing country context like Uganda's. By strengthening foundational ICTs and aligning infrastructure strategy with institutional mandates, governments can build digital systems that are not only functional, but trustworthy and resilient.

8. REFERENCES

- Heeks, R. (2006). *Implementing and managing eGovernment: An international text*. Sage Publications.
- Heeks, R. (2018). *Information and communication technology for development (ICT4D)* (2nd ed.). Routledge. <https://doi.org/10.4324/9781315737490>
- International Telecommunication Union. (2020). *Digital government and ICT infrastructure: Building resilient public services*. ITU Publications.

- Kettani, D., Moulin, B., & Elmahdi, A. (2014). *E-government for good governance in developing countries: Empirical evidence from Africa*. Springer. <https://doi.org/10.1007/978-3-319-03125-3>
- National Information Technology Authority-Uganda. (2019). *National information technology policy*. Government of Uganda.
- National Information Technology Authority-Uganda. (2020). *Digital transformation roadmap for Uganda*. Government of Uganda.
- OECD. (2020). *Digital government index 2019: Results and key findings*. OECD Publishing. <https://doi.org/10.1787/4de9f5bb-en>
- Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.
- United Nations. (2020). *E-government survey 2020: Digital government in the decade of action for sustainable development*. United Nations Department of Economic and Social Affairs.
- United Nations Development Programme. (2018). *Digital strategy 2019-2021*. UNDP.
- World Bank. (2016). *World development report 2016: Digital dividends*. World Bank Publications. <https://doi.org/10.1596/978-1-4648-0671-1>
- World Bank. (2020). *GovTech: Putting people first*. World Bank Group.
- Yildiz, M. (2007). E-government research: Reviewing the literature, limitations, and ways forward. *Government Information Quarterly*, 24(3), 646-665. <https://doi.org/10.1016/j.giq.2007.01.002>

9. APPENDICES

Appendix A: Ethical and Confidentiality Considerations

Given the sensitivity of financial and government data handled by MOFPED, strict confidentiality was maintained throughout the study. No system credentials, classified configurations, or security-sensitive details are disclosed in this report. Findings are presented at an aggregate and descriptive level to avoid exposing vulnerabilities or identifiable operational weaknesses.

Participation in interviews was voluntary, and respondents were informed that the information collected would be used solely for academic purposes within the Master of Science in E-Governance Technology and Services program.

Appendix B: Summary of Interviewed Functional Units

Interviews and discussions were conducted with representatives from the following units within MOFPED:

- Security Team
- Networking Team
- Hosting and Infrastructure Team
- Applications Team
- Service Desk Team
- Supervisory and Management Personnel within MIS

These units were selected based on their direct involvement in the planning, operation, and governance of digital infrastructure supporting e-governance initiatives at the Ministry.

Appendix C: Apprenticeship Context and Learning Environment

The research was conducted during an e-governance apprenticeship undertaken within the MIS Department at MOFPED. The apprenticeship provided hands-on exposure to real-world infrastructure operations, including system maintenance, incident handling, inter-team coordination, and interaction with external stakeholders such as NITA-U and system vendors. This embedded learning environment enabled me to observe both formal processes and informal operational practices that are often absent from official documentation. The apprenticeship context strengthened the validity of the study by grounding analysis in lived institutional experience rather than abstract assumptions.

Telephone: 256 41 707000/232095
Fax : 256 41 4233524
Email: finance@finance.go.ug
treasury@finance.go.ug
Website : www.finance.go.ug
Plot No. 2-8 Sir Apollo Kagwa Road
In any correspondence on
This subject please quote No. **HRM 140/170/04**



Ministry of Finance, Planning &
Economic Development,
P.O. Box, 8147
Kampala, Uganda

13th October, 2025

Mr. Kafuko George Hillary
Makerere University
Tel: 0770805281

ADMISSION FOR APPRENTICESHIP

This is to inform you that you have been offered an opportunity to undertake apprenticeship training in the Ministry for a period of **12(Twelve) Weeks w.e.f 20th October, 2025 to 10th January, 2026.**

During the period of apprenticeship, you will be attached to the Management Information Systems Department under the supervision of the Acting Commissioner, Management Information Systems Department.

Please take note that the Ministry has granted this offer to you on understanding that this is not an employment opportunity, but part of your learning process and the Ministry shall not be responsible for any costs associated with your participation in the apprenticeship, except for guidance as may be deemed necessary. You will be expected to produce a report at the end of your apprenticeship, a copy of which shall be retained by the Ministry for future reference.

Your attention is drawn to Section J-f of the Uganda Public Service Standing Orders relating to enhancing employability skills of graduates from training institutions. You will be further expected to abide by all Ministry rules, regulations and the code of conduct binding to all employees in public offices.


Richard Patic Bbosa
For: PERMANENT SECRETARY/SECRETARY TO THE TREASURY

Cc. The Ag. Commissioner
Management Information Systems Department

Mission
"To formulate sound economic policies, maximize revenue mobilization, ensure efficient allocation and accountability for public resources so as to achieve the most rapid and sustainable economic growth and development"

Appendix D: E-Government Apprenticeship Questionnaire

This study was informed by a structured questionnaire developed to guide learning engagements with technical and managerial teams within the Ministry of Finance, Planning and Economic Development (MOFPED). The questionnaire was designed to capture practical insights into how digital infrastructure supports e-governance operations across different functional units.

The questionnaire covered the following thematic areas:

- Information security practices and risk management
- Network architecture and connectivity management
- Hosting, data centre operations, and disaster recovery
- Application support and system interoperability
- Service desk operations and user support mechanisms
- Governance, coordination, and the role of external partners

The instrument was administered through semi-structured interviews with selected staff within the Management Information Systems Department. Its design ensured consistency across engagements while allowing flexibility to explore context-specific issues raised by respondents.

E-Government Apprenticeship at the Ministry of Finance, Planning and Economic Development (MOFPED)

Questionnaire

Prepared By: *George Hillary Kafuko, Master E-Governance Technology & Services (METS) Program at Makerere University*

Purpose: This questionnaire is meant to guide discussions and learning engagements with the different technical teams under the Ministry's E-Government function. The goal is to better understand how each communicated unit supports digital service delivery, infrastructure security, and overall e-governance within MOFPED.

1. Security Team

Objective: *To Understand how the ministry secures its systems, data, and users while balancing compliance and accessibility.*

1. Kindly walk me through how the security team supports the rest of the IT functions within the ministry?
2. What are the most common security challenges you face in protecting financial and government data?
3. How do you handle incidents or attempted breaches? Is there a formal response process?
4. What measures are in place to ensure users maintain good cybersecurity practices?
5. How do you balance user convenience and system security, especially for high-privilege accounts?
6. Are there any upcoming improvements or projects aimed at strengthening the ministry's security posture?
7. How does the team stay updated on new security risks or technologies relevant to government operations?

2. Service Desk Team

Objective: *Understand how user support and service management contribute to smooth ministry operations.*

1. What types of issues do you most commonly receive from users across departments?
2. How does the team track and prioritize service requests or incidents?
3. Is there a Service Level Agreement (SLA) or response target that guides your operations?
4. How do you handle recurring issues or system outages to avoid repetition?
5. What tools or systems are you using for ticket management and communication with users?
6. How does the service desk coordinate with other teams like Applications or Networking when incidents overlap?
7. From your experience, what are some small process improvements that could make user support more efficient?

3. Hosting Team

Objective: *Learn how infrastructure, servers, and hosted applications are managed and maintained.*

1. What systems or applications are hosted internally versus externally (e.g., cloud or NITA-U data center)?
2. How do you ensure reliability, uptime, and redundancy for hosted systems?
3. What's the general backup and disaster recovery approach for critical systems?
4. How do you monitor performance and resource usage across hosted environments?
5. Are there any challenges you face in terms of hardware capacity or integration with other MDAs?
6. How does the team plan for upgrades or new deployments without disrupting service?
7. From your perspective, what are the key considerations when deciding what to host in-house versus outsource?

4. Applications Team

Objective: Explore how digital solutions management and applications support financial management and public service delivery.

1. Kindly give me a quick overview of the main applications you manage or support here at the ministry?
2. How does the team handle application updates, testing, and version control?
3. What's the typical process when a department requests a new system or feature?
4. How do you ensure interoperability with other government systems especially from MDAs that exchange data with MOFPED?
5. Are there any in-house applications developed locally, or do you mostly work with vendors?
6. What challenges arise when integrating applications with older systems or manual processes?
7. What would you say are the key success factors when rolling out a new digital service internally or nationally?

5. Networking Team

Objective: Understand how the ministry's communication and connectivity backbone supports e-governance.

1. What's the general network architecture like, and do you connect directly to the NITA-U backbone or have independent links?
2. How do you ensure stable connectivity across all ministry offices and remote sites?
3. What monitoring tools are used to detect or troubleshoot network performance issues?
4. How do you manage user access across different subnets or VLANs to maintain security?
5. What's the process for network upgrades or expansion when new systems are introduced?
6. How does the team collaborate with the Security and Hosting units to ensure seamless service delivery?
7. In your view, what are the main bottlenecks or areas that could improve network efficiency at the ministry?

6. General Questions - supervisors/Managers

1. How do all these teams collaborate when implementing new digital or e-government initiatives?
2. What governance or coordination structure exists to align IT activities with the ministry's broader goals?
3. How do you ensure business continuity and minimize downtime across departments?
4. What role do external partners (like NITA-U, World Bank, or service vendors, etc) play in supporting your ICT initiatives?
5. What lessons or practices could be shared with other MDAs to strengthen government-wide e-governance?

Link to the Websites & Portals Evaluation: <https://forms.cloud.microsoft/r/17SP6sR32d>