State of Palestine

Ministry of Local Government

# Digitalization Strategy in the Local Government Sector

# (2025-2030)

May/2024

## Preface

Pursuant to the priorities of the nineteenth Palestinian government, including the implementation of a reform program and performance development for governmental institutions, all the way to a governance system that guarantees good governance and improves the performance and services in all sectors. Building upon the efforts of previous Palestinian governments in the field of digital transformation, and in line with Palestine Digital Agenda 2030, and all associated policies, strategies and efforts, the Digitalization Strategy in the Local Government Sector constitutes a referential foundation for digitalization at the level of local government sector.

The local government sector is one of the most important sectors that provides services to citizens, especially through LGUs and their functions. In this context, the Ministry of Local Government, due to its guiding and supervisory nature over the sector, is keen on drawing policies and devising strategies that support enhancing efficiency, the quality of provided services and transparency, in a manner that realizes citizen welfare.

This strategic document shows the degree of synergy among partners in the sector and those who collaborated in its development. It also shows the keenness to achieve progress in digitalization at the local level in order to keep up with digitalization at the national level and the accelerated technological advancement in accordance with the best practices.

I would like to express my gratitude and appreciation to all those who contributed to the development of this strategy, which will be a reference for the upcoming period for the Ministry, the MDLF and APLA, as well as the remainder of local government units (LGUs), and for the programs and projects targeting the digitalization of the sector.

**Dr. Eng. Sami Hijjawi**

**Minister of Local Government**

Index:

## Abbreviations:

| Abbreviation | Description |
|---|---|
| Team | The team who prepared the Digitalization Strategy in the Local Government Sector, formed pursuant to the decision No. (1-2023-3254) issued by H.E Minister of Local Government on May 10, 2023. |
| MoLG | Ministry of Local Government |
| APLA | The Association of Palestinian Local Authorities |
| MDLF | Municipal Development and Lending Fund |
| MTDE | Ministry of Telecommunications & Digital Economy |
| PESTEL | Analysis of Political, Economic, Social, Technological, Legal and Environmental external factors |
| SWOT | Analysis of Strengths, Weaknesses, Opportunities and Threats |
| INDIGO | Inclusive Digital Governance Program |
| HCD | Human Centred Design Methodology |

## Executive Summary

The National Digital Strategy 2025-2030 constitutes a guiding and indicative basis for Palestinian local government units (LGUs) and all partners in the local government sector, in order to realize its digitalization, enhance and develop public services provided to citizens. At its core, it relies on a set of key elements aiming to consolidate the basis for an inclusive and efficient digital local government sector, enhancing LGUs' capacity to respond to the various citizens' needs and strengthen their resilience. Moreover, it stimulates sustainable development in Palestine in line with the government's national vision for digitalization, contributing to the enhancement of the local government sector's role in achieving that vision.

The strategy comprises of several main goals, including enhancing digital infrastructure and technological tools, building capacities, and enhancing the management of change through working on enhancing the culture of digitalization, educating LGUs and their entire staff on raising awareness of local communities. It seeks to enhance digital resilience and guarantee continued basic services without interruption, especially in cases of emergency. Such goals are the guiding foundation for efficient and effective implementation, as it was based on analyzing the status quo of the local government sector concerning digitalization, by focusing on studying the strengths, weaknesses, opportunities and threats (SWOT analysis).

The strategy also includes the main principles and pillars, which serve as a basis that contributes to the continued digitalization process, in addition to the values and principles guiding that process, such as transparency, inclusion, and sustainability based on a human centered design, with the aim of achieving long-term effective results.

The Digitalization Strategy in the Local Government Sector indicates the measures, procedures and interventions to be implemented to realize effective transformation, by devising a detailed framework that clarifies how to achieve the desired goals and transform all challenges into opportunities in order to realize our ambitious vision for an effective and comprehensive digital local government sector. The framework includes planning, allocation of resources, training cadres and staff, implementing optimal digital technologies, identifying the key dimensions for implementing the strategy, and setting up a timeframe for effectively achieving the goals and objectives. Moreover, the strategy covers the monitoring and evaluation process through effective mechanisms for monitoring the implementation processes, regularly assessing performance to guarantee achieving the desired goals, and continuously improving the process.

## Introduction:

The successive Palestinian governments paid special attention to the welfare of Palestinian citizens and improving their quality of life. Technology is a critical tool for this endeavor. As such, the interest of the Palestinian government in pushing the wheel of digitalization is increasing at both, national and local levels, in order to develop governmental services making them more efficient and effective, which allows citizens easy access to such services.

Due to its supervisory and guidance nature over the local government sector, the Ministry of Local Government (MoLG) enjoys a pioneering status in leading the journey of digital transformation in the sector. Since its inception, MoLG was keen on achieving the optimal utilization of information technology (IT) to enhance the services provided to citizens, which was embodied in the following tangible steps: fund raising, partners' guidance, devising policies and strategies, and implementing projects that make advancements in the digital transformation and digitalization of Palestinian LGUs.

In coordination and collaboration with various active players, MoLG launched a strategic initiative for developing a comprehensive framework for transforming LGUs into e-municipalities covering 2019-2023. The Ministry, the Municipal Development and Lending Fund (MDLF), the Association of Palestinian Local Authorities (APLA) and several other donors working on issues of digital transformation officially adopted the framework.

Ministry's efforts in digitalization are in line with the national vision and coincide with the Palestinian government launching Palestine Digital Agenda 2030, the adoption of the Digital Government Strategy and its Roadmap (2024-2029), and developing the National Policy for Digital Accessibility. These efforts are the result of fruitful partnerships with various active players in the local government sector, particularly the MDLF. These partnerships contributed to realizing tangible achievements, starting with the Spatial Data Infrastructure (SDI) and (Geomolg) system, as well as the development of several systems for LGUs such as the integrated financial management systems, all the way to the public services center and its associated technological tools.

In light of the accelerating technological advancement globally and nationally, and with the Strategic Framework for Transforming LGUs into E-municipalities, approaching its closing date by the end of 2023, the Ministry and partners in the sector saw an urgency for developing a strategy for the digitalization of the local

government sector. The new strategy must be in line with national agendas and policies in the area of digitalization, and that meets the requirements of digital transformation at the local level over the period (2025-2030). Therefore, it was decided to form a specialized team delegated with developing the Digitalization Strategy in the Local Government Sector, comprised of representatives of different stakeholders, most importantly:

1. Ministry of Local Government (MoLG)
2. Ministry of Telecommunications & Digital Economy (MTDE)
3. General Secretariat of the Council of Ministers
4. The Association of Palestinian Local Authorities (APLA)
5. The Municipal Development and Lending Fund (MDLF)
6. Academia Sector in Gaza Strip/ University College of Applied Sciences
7. Birzeit University
8. An-Najah National University
9. Palestinian Information Technology Association of Companies (PITA)
10. The Palestinian Information & Sciences Technology Syndicate (PALIST)
11. E-Governance Project (INDIGO) funded by GIZ
12. Municipality of Nablus
13. Municipality of Hebron
14. Municipality of Beitunia

The Team's methodology:

- Conducting periodic meetings to present implemented steps and monitor advancement.
- Reviewing all documents relevant to digital transformation and digitalization at all, local, regional and global levels.
- Assessing the current reality of information technology in the local government sector.
- Forming focus groups throughout the different stages of the team's work.
- Drafting strategies, reviewing and accurately editing them.
- Obtaining feedback and making the necessary modifications to the draft strategy.
- Adopting the strategy by the team and endorsing it to H.E. Minister of Local Government for final approval.

## Definitions and Concepts:

**Citizen quality of life from the local government perspective:**
Enabling citizens to obtain services of the local government sector easily, with quick responsiveness, high efficiency and lower cost.

Citizens from the perspective of the National Digital Strategy in the Local Government Sector:

Every taxpayer or recipient of services from the local government sector regardless of her/his gender, age, place of residence or disability.

**E-Municipality:**

A system based on transforming the way LGUs work (including municipalities and village councils) as well as joint service councils through the optimal and efficient utilization of information and communication technology (ICT) with the aim of enhancing service management and delivery to citizens to enhance the realization of the concepts of good governance.

**Human Centered Design (HCD):**

An innovative approach for overcoming challenges integrating the needs of citizens, their experiences, requirements and aspirations at the center of the problem solving process, based on "learning by experience" experimental, creative, participatory and repetitive means, in order to guarantee devising innovative solutions for whom they are designed.

**Digitalization:**

A process of transforming information and data from a format relative to humans to a digital form that can be stored and processed using numbers (binary or decimal). This includes, transforming images, audio, text, video and other forms of data into forms that can be comprehended and processed by digital systems. Digitalization is a means of business development by using digital solutions.

**Digital Municipality:**

Is an electronic municipality that uses technology at an inclusive and wide scale for all the municipal activities and services, contributing to further improving citizens' quality of life.

## Digital transformation at the national level:

Since the dawn of establishing the Palestinian National Authority, the State of Palestine sought effortlessly to build institutions that are up to date with the global best practices, and so focused on computerizing its processes. With the emergence of the concept of e-government, for more than fifteen years, successive Palestinian governments have adopted the idea of transforming into an e-government, due to their understanding of its impact on providing better services to Palestinian citizens and enhancing the efficiency of governmental work. Therefore, it has devised and implemented several plans, capacity building programs, policy papers, strategies and projects that serve the transformation process and contribute to achieving its goals. Several projects in the field were implemented including the Governmental Network, National Data Transfer, Zinnar, e-government services system "Hukumati", the Electronic Transaction Law, the law regulating the governmental e-services system and the Cybercrime & ICT crimes Law.

Believing in the importance of digital transformation and its role in realizing sustainable development in Palestine, and building upon the efforts made in enhancing the e-government, the State of Palestine developed Palestine Digital Agenda 2030, and launched a group of strategic initiatives to fast forward the pace of digital transformation at a national level. The Digital Government Strategy 2024-2029 was adopted and circulated to all governmental departments to initiate the implementation of the roadmap emerging from it, in addition to the national policy for digital accessibility.

The following documents constitute the key references at the national level for the Palestinian digital transformation process:

1. Law by Decree No. 11 of 2023 concerning the Governmental E-Services System.
2. Law by Decree No. 15 of 2017 concerning Electronic Transactions.
3. Palestine Digital Agenda 2030/ Council of Ministers' Resolution No. (13) of 2023.
4. Digital Government Strategy and its emerging Roadmap 2024-2029/ Council of Ministers' Resolution No. (11/249/18/M.W/M.A) of 2024.
5. Information Security Management/ Council of Ministers' Resolution No. (12) of 2023/ Amending Council of Ministers' Resolution No. (6) of 2020.
6. Hosting institutions on the cloud and linking it to the National Data Transfer/ Council of Ministers' Resolution No. (06/151/18/M.W/M.A) of 2022.

7. The Governance Manual of Governmental E-services and Financial Policy for E-payment/ Council of Ministers' Resolution No. 03/127/18/M.W/M.A of 2021.
8. Amended Information Security Policy/ Council of Ministers' Resolution No. 09/122/18/M.W/M.A of 2021.
9. National Policy for Digital Transformation/ Council of Ministers' Resolution No. 17/105/18/M.W/M.A) of 2021.
10. Strategic Framework for Transforming into E-Municipalities (2019-2023)/ Ministry of Local Government – November/2018.
11. The Manual for Developing IT Policies in LGUs (2022-2023)/ Ministry of Local Government.

## Vision – Goals:

**Vision:**

Effective and comprehensive digital local government sector that enhances the welfare of beneficiaries and stimulates sustainable development in Palestine.

**General purpose:**

Advancing the quality of services provided to citizens in the local government sector through adopting a comprehensive methodology for digitalization that focuses on the needs of citizens and contributes to achieving digital transparency, accountability and inclusion, as well as quick response.

**Strategic goals:**

1. Enhancing digital infrastructure and technological tools:
   Providing a safe and reliable technological environment capable of providing digital services and guaranteeing its continuity through building and enhancing technological infrastructure and its associated tools and systems among all partners in the local government sector, as well as using digital tools and automation to enhance administrative processes.
2. Building capacities and enhancing the management of change:
   Developing digital skills and capacities necessary for all individuals working in the local government sector, as well as implementing the best practices in management of change in service of digital transformation.
3. Enhancing digital culture and community:
   Working on spreading the culture of digitalization and educating local communities and the cadres working in the local government sector on the importance of digital transformation and the means of achieving it, which contributes to enhancing confidence in digitalization, and motivating the society to apply and use it.
4. Enhancing digital resilience:
   Applying risk management, providing plans and tools for recovery from disasters, developing resilience strategies and alternative plans to guarantee the undisrupted provision of basic services in cases of emergency, as well as capitalizing on digital platforms and remote work solutions to maintain continuity of work.

## Analyzing current reality of the local government sector in the area of digital transformation:

A comprehensive survey to assess the reality of information technology (IT) in the local government sector was conducted during the first half of 2023. The survey targeted all components of the sector, including LGUs, MoLG, MDLF, and APLA. Annex (1) provides a detailed analysis of the reality of local government sector in the area of digital transformation. Results can be summarized as follows:

### First: Assessing the reality of IT in LGUs:

1) **Digital infrastructure and computerized systems:**
Digital infrastructure, computerized systems and its associated IT tools are available, as well as partial availability of internal digital services, and in-house hosting of systems. The survey showed that 55.8% of LGUs have digital infrastructure and computerized systems to a moderate degree and 44% have internet services and in-house hosting of systems. Moreover, there is a general lack of disaster recovery centers.
2) **Digital services:** Survey showed that 79% of LGUs lack availability of digital services or have digital services but with a poor level. Moreover, 15% of LGUs have moderate digital services. However, in terms of websites, 44% of LGUs have official websites and 15% do not have any official web pages.
3) **Data privacy and information security:**
A total of 47.7% of LGUs take into consideration and focus on maintaining the privacy of data and have information security systems, meanwhile 37.2% do not have such systems or are available in very primitive forms. However, concerning risk assessment, the survey showed that 50% of LGUs did not conduct any form of risk assessment through a third party.
4) **IT Planning and cadre development:**
The area of IT planning and cadre development suffers a 58.1% shortage, due to several reasons, most importantly lack of allocation of required budgets. There is also a shortage in citizen participation in most of LGUs in the development of digital transformation strategies. Only 37.2% of these LGUs have active strategies, dedicated budgets and cadres in the area of IT.
5) **Cooperation and participation:** the results shows shortcomings in the area of quadripartite innovation (private sector, academia, LGUs, regional and international organizations), which may hinder the implementation of the national digital strategy at the level of local government. The survey shows that 42% of LGUs have no collaboration with the private sector and only 22%

have limited collaboration. In 81% of LGUs, there is no collaboration with Academia, and the percentage reaches 83% in relation to collaboration with the local communities. Meanwhile, lack of collaboration or cooperation between LGUs, regional and international organizations reached 86%.

6) **Training and performance appraisal:** it appears that 86% of LGUs do not have any mechanisms for training and performance appraisal. The survey shows that 54.7% of LGUs do not have any means, and 31.4% have means that can be classified as extremely poor. The study also showed that only 2.3% of LGUs have effective means for training and performance appraisal.

**Results analysis:**

Relations between the different variables have been further analyzed with the aim of acquiring additional observations and results. General information variables related to the governorates, classification of LGUs, number of staff members, and the status of digitalization were processed using crosstab. Annex (1) shows the detailed analysis.

**The impact and implications of the results of LGUs' analysis on the Digitalization Strategy in the Local Government Sector**

- Despite the availability of good computerized systems and accessories, and good internet connectivity in LGUs, there is a lack of necessary foundations such as data centers and data retrieval centers matching the e-services provided to citizens, and enhancing LGUs' work. Therefore, it is preferable to establish these data centers, and to take advantage of existing centers as an auxiliary alternative or as data retrieval centers.
- E-services are poor or absent in all classifications, although making it available to citizens must be smooth, undisrupted, and available instantly. Furthermore, these services should be linked to a central government to facilitate accessibility and processing, which must be part of the structure of LGUs' annual plans.
- Survey shows that 63% of municipalities suffer weaknesses in the cadres of IT, planning and development in all four classifications as well. Therefore, this issue ought to be considered seriously in the annual plans to fast track the digitalization process in all LGUs.
- Furthermore, mechanisms of participation, cooperation, collaboration, training and performance appraisal systems are poor in all LGUs of all classifications. This requires a serious commitment from MoLG, MDLF and APLA, so that these parties may play their role in combating these issues and nurturing the digital

transformation project as part of the systematic planning and work towards providing e-services smoothly to citizens and LGUs' employees.

## Second: Assessing the reality of IT at the national level of the sector:

### (MoLG, MDLF and APLA)

Based on the extrapolation of the reality of MoLG, MDLF and APLA, and by answering certain questions related to infrastructure, networks, communication, information security, data management, services, maintenance and cadres, the following was concluded (details available in Annex (1)):

**IT infrastructure:**

IT infrastructure in each of the three institutions (MoLG, MDLF and APLA) is considered capable of meeting their current needs, while emphasizing the need for continuous improvement and development of infrastructure, especially in the field of information security, use of the cloud, backups and disaster recovery sites.

**Networks and communications:**

Networks and communications in the three institutions are considered the key pillar for internal communication with its staff and services. Continuous development of networks and communications is considered an urgent need to keep up with the fast advancement in technology, as it is considered a key pillar for institutions' work.

**Information security:**

The three institutions pay significant attention to information security issues in order to protect its information from security threats, which requires effective periodic plans to guarantee the protection of systems and data, in addition to external sources ensuring its retrieval effectively. There is a permanent need for security awareness courses in these institutions, which take into consideration the developments in the security field.

**Data management:**

Most of the data in the three institutions is managed through special information systems linked to databases or file systems. The study shows that the majority of systems used for data management are at a high degree of efficiency and reliability, and that consider the required bases for data management, especially with regards to data accessibility permissions, data safety and backups.

**Service management and maintenance:**

Services and required maintenance in the field of IT, whether in relation to infrastructure, systems or programs, are provided through the IT staff in the three institutions as well as external providers of support and maintenance services, depending on the type of service and the nature of required maintenance.

**IT Staff:**

MoLG has a general directorate for IT, with a permanent staff of 7 specialists working at MoLG H.Q. who currently cover services at the level of the Ministry and its Directorates. Meanwhile, MDLF has two employees, and APLA has only a part time employee. This indicates the need for completing recruitment of personnel in the three institutions, taking care of their training and capacity building.

**SWOT Analysis:**

A SWOT analysis of the internal and external environment of the local government sector was carried out at the level of MoLG, MDLF and APLA, which shows a distinctive advancement in using IT in addition to different gaps in each institution separately, which can be summarized as shown in the table below:

| Strengths | Weaknesses |
|---|---|
| **Ministry of Local Government (MoLG)** | **Ministry of Local Government (MoLG)** |
| 1. Availability of servers and infrastructure in the Ministry's premises provides full control of the systems and data, which increases security and control.<br>2. Using modern technologies: the use of Blade Servers and VMware allows division of resources efficiently and effectively.<br>3. Using firewalls, anti-virus software and data protection systems contributes to enhancing data security.<br>4. Distributing the load and compiling data: using compilation technologies on servers and distributing the load guarantees sustainability and efficiency of systems. | 1. Lack of security education: lack of training courses or workshops for enhancing security awareness among employees, may leave the Ministry vulnerable to security threats.<br>2. Lack of systems for detecting breaches: lack of systems for detecting breaches may leave the Ministry vulnerable to undetected attacks.<br>3. Lack of emergency plans: lack of emergency plans for facing the disruption of services or cyber-attacks may increase its adverse impact.<br>4. Management of manual maintenance: relying on the manual management and maintenance of computers and software |

| | |
|---|---|
| 5. Data types: the ability to use and manage a wide spectrum of data types enhances the Ministry's flexibility in processing data.<br>6. Data management systems: using data management systems helps guarantee the quality of data and its effective organization.<br>7. Backup processes: conducting periodic backup and data retrieval processes contributes to achieving data sustainability and ensuring against its loss. | may be ineffective and increases the margin of human error.<br>5. Lack of specified update and upgrade policies: lack of specific policies for the updating, upgrading and maintenance processes may lead to delays in infrastructure enhancement. |
| **The Association of Palestinian Local Authorities (APLA)** | **The Association of Palestinian Local Authorities (APLA)** |
| 1. Cloud storage: relying on cloud storage provides APLA with the flexibility and ability to expand the storage capacity in a quick and efficient manner.<br>2. Applying clear data access permissions reduces the risk of leaks and unauthorized access.<br>3. Using effective means of protection at APLA such as servers' access permissions.<br>4. Using strict data access permissions with employees.<br>5. Using effective internal and external data backups.<br>6. Effective and periodic network monitoring processes.<br>7. Controlling the quality of data and verifying its safety and integrity.<br>8. Periodic checking of backups.<br>9. Periodic courses to increase awareness on information security among employees.<br>10. Using a hybrid system for services and data. | 1. Having a small number of servers at APLA's office and the significant reliance on cloud storage.<br>2. Using the File System extensively with simple use of data management systems such as MySQL and Oracle.<br>3. Lack of systems for managing the maintenance files and upgrading software may lead to missing periodic maintenance and system upgrades.<br>4. Having a part time IT employee may increase delays in dealing with technical issues.<br>5. There are no specific plans and policies for managing the IT infrastructure and continuous upgrading.<br>6. Lack of mechanisms for checking the backups retrieved from the e-cloud.<br>7. Making backups of data only, without the software used at APLA. |
| **The Municipal Development and Lending Fund (MDLF)** | **The Municipal Development and Lending Fund (MDLF)** |
| 1. Using e-clouds provides flexibility and the ability to access data from anywhere and at any moment.<br>2. A hybrid infrastructure that combines local servers and e-clouds provides flexibility and sustainability when uploading data and in cases of emergency.<br>3. Using an advanced operating system with partition systems (VMware) increases the efficiency of servers and utilization of resources. | 1. Lack of training targeting employees: lack of provision of security awareness courses to employees increases the risk of cyber-attacks.<br>2. Lack of a standardized system for equipment and devices management and maintenance may lead to loss of data or disruption of services in case of poor coordination.<br>3. Lack of specific policies for managing updates, upgrades and their timing: it fully |

| | |
|---|---|
| 4. Capitalizing on data dissemination and compilation technologies and auto upload of backups contributes to enhancing safety and continuity of work.<br>5. Encrypting data and applying the permissions system enhances data security and prevents unauthorized access.<br>6. Using the expanded detection and response system (XDR) to detect security threats enhances MDLF's ability to face cyber threats.<br>7. Continuous upgrading of infrastructure: the ability to upgrade infrastructure and use IT increases efficiency of work and data security.<br>8. Using security systems: using firewalls and the various security systems enhances information security and the detection of unsafe activities linked to data and the internal network. | relies on updates from Microsoft exclusively. |
| **Opportunities** | **Threats** |
| **Ministry of Local Government (MoLG)** | **Ministry of Local Government (MoLG)** |
| 1. Enhancing security awareness: the ability to provide training courses and workshops to employees enhances their security awareness and their skills in the field of information security.<br>2. Development of intrusion detection systems: the ability to enhance the safety structure by implementing intrusion detection systems to monitor and respond to cyber-attacks.<br>3. Using intrusion detection software such as Cisco NGIPS and Fidelis Network.<br>4. Using intrusion detection devices such as FireEye Intrusion Prevention System and Hillstone S-series.<br>5. Storing data on the cloud: increased use of cloud storing and data encryption may enhance securing data and responding to the changing needs.<br>6. Enhancing maintenance and updates: the ability to organize the maintenance and | 1. DDoS attacks: type of attacks that may adversely affect the stability of services, which requires the development of preventive strategies and effective response.<br>2. Lack of emergency planning: in cases of crises, lack of emergency plans may leave the Ministry vulnerable to disruption of work and loss of data.<br>3. Insufficient safety: lack of using advanced safety systems (WAF for example) makes the infrastructure vulnerable to advanced security threats.<br>4. The chance of human error: relying on manual management allows opportunities for human error and delays in maintenance and updating.<br>5. Loss of data: lack of specific policies for updates may increase the risk of data loss.<br>6. Insufficient offline backup compared to best practices, systems and equipment that can be used to conduct data retrieval. |

| | |
|---|---|
| updating processes to enhance infrastructure performance.<br>7. Organizing processes: an opportunity to organize and guide the management of processes by applying the appropriate systems.<br>8. Capacity development: providing training courses for IT staff may help in developing their skills and increasing their awareness on information security.<br>9. Benefiting from the services provided by the Ministry of Communication and Digital Economy (MTDE) pursuant to the Council of Ministers' Decree No. 06/151/18 of 2022. | 7. Lack of coordination: lack of an IT employee in most of the directorates affiliated with the Ministry, may affect coordination between the Team and effective distribution of tasks. |
| **The Association of Palestinian Local Authorities (APLA)** | **The Association of Palestinian Local Authorities (APLA)** |
| 1. Using intrusion detection software such as Cisco NGIPS and Fidelis Network.<br>2. Using intrusion detection devices such as FireEye Intrusion Prevention System and Hillstone S-series.<br>3. Concerning data access permissions, they were developed through empowering data owners and enabling them to control the rights to access the data they own, in order to make sure that all processes are authorized.<br>4. Using multi-step verification techniques such as the two-factor authentication (2FA), which can protect against unauthorized access.<br>5. Data flow technologies might be applied to detect unexpected changes to data over time, whether big or unexpected changes. | 1. Basic security measures are applied only at the level of data access permissions without the utilization of advanced systems.<br>2. Relying on one part time IT employee constitutes a threat in cases of intrusions or leaks.<br>3. Relying on the service provider to encrypt data and choose data storage locations.<br>4. Lack of assessment of all applicable security procedures and policies and enhancing them in relation to the new security threats and developments.<br>5. Using Files System instead of the full use of data management systems.<br>6. Dependency on third parties: extensive reliance on a third party may provide them with the leverage to hold off service provision and therefore hinders work processes.<br>7. Lack of accurate organization of updating, upgrading and replacement processes may leave systems vulnerable to attacks or violations. |
| **The Municipal Development and Lending Fund (MDLF)** | **The Municipal Development and Lending Fund (MDLF)** |

| | |
|---|---|
| 1. Enhancing employees mentoring and training: providing employees with training in the field of information security and using systems that decrease the threat of cyber-attacks.<br>2. Enhancing the coordination of work among IT employees helps enhance responsiveness to technological issues and problems.<br>3. Enhancing data management and coordination between IT employees may increase work efficiency and coordination between projects.<br>4. The use of project management tools contributes to better tracking and maintenance of devices. | 1. Lack of specific policies for managing updates and upgrades may lead to delays in applying and implementing new technologies.<br>2. MDLF extensively relies on maintenance contracts with companies providing IT services, which exposes it to risks in case of lack of availability of such services.<br>3. Irregular updates: lack of specific policies for managing updates may cause the infrastructure to be vulnerable to security gaps. |

**Recommendations:**

**Recommendations were provided to overcome the shortcomings, bridge the gaps, and build on the strengths of each institution as follows:**

| MoLG | APLA | MDLF |
|---|---|---|
| • To implement advanced DoS protection systems.<br>• To develop attack response plans DDoS including early detection and quarantining of suspicious activities.<br>• To develop and implement comprehensive emergency plans including data retrieval, and in cases of emergency, to provide clear guidance to the teams.<br>• To organize periodic trainings for the teams based on emergency plans.<br>• To assess IT infrastructure, update and upgrade security systems in accordance with the best practices.<br>• To enhance raising awareness on information security among employees, and to develop safe use policies for systems and software.<br>• To adopt automated management systems for maintenance, updates and | • To enhance and expand safety measures, develop access permissions in line with the potential threats, and consider the use of advanced technologies such as multi-factor authentication.<br>• To devise specific plans for periodic technological and security updates, in a way that guarantees updating the operating systems, software and security patches.<br>• To periodically invest in intrusion and security audit tests to identify the gaps and weaknesses, and correct them before they are abused.<br>• To employ an IT officer on full time basis to be directly responsible for IT and data infrastructure and security, as well as control of and response to any security threats effectively.<br>• To verify availability of agreements and accurate contracts covering all aspects | • To organize periodic security awareness courses to all MDLF employees, including on updates related to information security and proper online behavior.<br>• To create in-house awareness campaigns to highlight common safety and security threats and safe behaviour via email and other digital resources.<br>• To enhance and allocate resources: allocating more resources to provide the support and tools necessary for IT employees.<br>• To create a joint approach and tools for project management and documenting maintenance works and fixing bugs.<br>• To develop and implement a standardized system for hardware management and maintenance and |

| | | |
|---|---|---|
| upgrades to reduce human error.<br>• To provide continuous training on maintenance and safety tasks to employee.<br>• To devise periodic policies for backup and data retrieval processes.<br>• To apply encryption and access control solutions to protect data from unauthorized access.<br>• To apply advanced intrusion detection systems to monitor any unauthorized activity within the infrastructure.<br>• To develop emergency plans including the immediate response to disruption of services or cyber-attacks and quick recovery of safety.<br>• To adopt automated management systems for the maintenance of hardware and software to enhance efficiency and decrease human error.<br>• To develop specific policies and timeframes for the updates and maintenance processes, and to regularly apply them. | of service provision such as issues of data encryption and appropriate storage and maintenance of data.<br>• To conduct a periodic assessment of applied security policies and procedures, and to enhance them in accordance with the new security threats and developments.<br>• To use advanced data management systems to increase safety and data organization.<br>• To apply tracking systems to emails and its components to detect any potential threats before it reaches to the employees' email.<br>• To devise a strategy for dealing with third party providers of e-cloud services including the revision of safety and security requirements in contracts and agreements. | guaranteeing its conformity with the safety policies.<br>• To create specific policies for managing updates and upgrades including the timeframes and test procedures.<br>• To develop a regular updates policy with periodic tests to guarantee the integrity of systems and applications.<br>• To prepare a plan for responding to security threats, including the procedures for dealing with potential attacks, in addition to circulating the plan to all employees and regularly updating it. |

## Key Principles and Pillars for Digital Transformation in the Local Government Sector

- **Principles**

1. Citizens are the main axis of the digital transformation process.
2. Governance, reliability and transparency.
3. Services provided by LGUs are accessible through a digital platform/s developed through the partnership that combines LGUs with partners, citizens and service providers.
4. Flexibility, sustainability and continuous enhancement and improvement.
5. Easy use, empowerment of beneficiaries, and enhancing the culture of digital transformation.
6. Guaranteeing data security and privacy.
7. The potential for interoperability and compatibility.
8. Guaranteeing the potential for expansion and continuity.
9. Moral principles and justice.
10. Realistic and applicable.

- **Key Pillars:**

1. National strategies and policies related to digital transformation.
2. The Human Centered Design (HCD).
3. Cooperation and complementarity of efforts.
4. Technical and administrative development.
5. Accumulation of experiences and skills.
6. Availability of digital transformation resources and requirements.
7. The management of change.
8. Risk management.

## The methodology of digital transformation in the local government sector:

The digitalization strategy in the local government sector is of great importance in terms of providing the foundation and reference for achieving transformation towards digital LGUs. Components of the strategy, including the goals, principles and bases are considered a key and reliable determining factor in the implementation process, and for finding and developing the means and solutions necessary for achieving the desired development. The reality analysis of LGUs in the area of digital transformation revealed a clear discrepancy among LGUs in terms of transformation, which emphasizes the importance of having these strategies and adopting them as a key element for measuring progress in the digital transformation of LGUs.

Based on the analysis of the current reality of LGUs, taking into consideration the experiences acquired from others and the best practices followed, the need for adopting a special methodology for digital transformation in the local government sector is evident. The methodology may be called "Methodology of stages, gradualism and continuous improvement", given that includes all fields necessary for transformation. Such fields include:

1. Transformation of procedures and processes: signs of transformation in this regard include simplifying and shortening the procedures and processes conducted by LGUs to enhance citizens' quality of life.
2. Transformation in the accuracy of information and administrative tools to control information.
3. Transformation in the use of technology: signs of transformation in this regard include the availability of sustainable investments in ICT to establish flexible infrastructure with open architectures.
4. Transformation in the culture of LGUs and individuals: signs of transformation in this regard include participant's understanding of the importance of her/his role in the total system, whether the participant was an individual or a department, and her/his eagerness to link her/his goals with the overarching goals of LGUs.
5. Transformation in community awareness and culture concerning the importance of benefiting from the e-services LGUs provide.

In general, the digital transformation process is a long-term and gradual process: LGUs determine their level of focus on each stage according to their own vision and mission, and in harmony with the public digital transformation strategies in the local government sector and the applicable national policies.

## Implementation Dimensions and Map:

In order to guarantee the implementation of the Digitalization Strategy in the Local Government Sector effectively, while considering its goals, principles and pillars, it becomes necessary to identify the key dimensions of the road map for implementing the strategy, which can be achieved as follows:

1. **Systems and software:**
   - Availability of effective systems and software as well as adaptation and harmonization of all LGUs works.
   - Availability of the systems and software required for protection.
   - Applying IT policies to the systems and software.
   - Availability of accurate data in the systems and software.

2. **Technological infrastructure:**
   - Availability of the devices and equipment required for the digital transformation process.
   - Availability of devices and equipment required for protection.
   - Availability of required communication lines and devices.
   - Applying IT policies including with regards to devices and equipment.

3. **E-services:**
   - Designing and developing e-services following the human centred design (HCD) methodology.
   - Annual and periodic updating of the services and procedures manual for LGUs.
   - Periodic assessment and continuous enhancement of the quality of e-services.

4. **Sustainability:**
   - Availability of systems and equipment for recovery from disasters.
   - Availability of a dedicated budget to guarantee the continuity of maintenance and the development of systems and devices.
   - Periodic assessment and updating of systems, programs, devices and equipment.
   - Availability of IT policies approved and adopted by LGUs.
   - Capacity building by training the cadres of LGUs.

5. **Trust and Culture:**
   - Awareness programs for the cadres of LGUs.
   - Awareness programs and campaigns for citizens.

- Adopting and applying incentives for the use of e-services.
- Applying the best practices and policies related to protection of personal data.
- Availability of effective means for monitoring and supporting the provision of e-services.

To develop a roadmap for implementing the strategy, we developed specific stages for implementation and making progress in achieving the strategic goals and working on the main dimensions of the digital transformation process. The following are the main stages of the roadmap, taking into consideration that it is possible to implement more than one stage simultaneously depending on the reality of LGUs:

1. **First stage: Enhancing the performance of internal services and interlinking computerized systems.**
   This stage is distinguished with computerized internal work procedures that realize quick response and accuracy of information in preparation for launching effective and reliable e-services. Moreover, it includes applying a single sign on system, in a way that guarantees the maximum accuracy and enhanced mechanisms used in services and the complaints system, while making sure the procedures followed by LGUs refer to procedural manuals and systematic audits in order to guarantee accuracy of information to be used in the next stage.

2. **Second Stage: Building capacities and enhancing the management of change and resilience to guarantee the continuity of services.**
   This stage aims to enhance the management of change within LGUs, training and education of LGUs' council members and employees on the importance of digitalization to enhance citizens' quality of life. This includes studying the degree of infrastructure information and technical readiness of LGUs, analysing gaps, identifying needs, and the scale of required work. In addition, systems and tools required for achieving the enhancement of digital resilience are taken into consideration in cases of disasters and climate events. Accuracy rate of technical information of LGUs is calculated based on an institutional analysis to be carried out, availability of an action plan with identified responsibilities and a timeframe for implementing each plan, and a methodology for implementation monitoring and evaluation. Among those plans is creating IT policies for LGUs and the plan for supporting resilience.

3. **Third Stage: Enhancing external e-services and enhancing citizen digital tools.**

Participation of citizens and stakeholders in the designing of digital services is considered a key factor in the success of launching digitalized services through trusted tools that enhance confidence in it and facilitates its use, allowing citizens to deal with all services and financial transactions with LGUs. Moreover, it enhances the implementation of the single sign on method for LGUs at the intermediate and long terms, in line with the national level concerning single sign on.

4. **Fourth Stage: Enhancing community culture in order to realize a resilient digital society.**
   This stage aims to enhance community culture. It involves meetings, conducting public polls, and adopting transparency in applied procedures, as there is a paramount importance in publishing budgets and engaging the local community through digital awareness activities and collaborative workshops targeting the public. This includes conducting specialized administrative training courses for relevant LGUs' staff, especially those working in the field of information and communication technology (ICT) on the optimal use of modern technology.

**Connections between the goals and implementation dimensions and stages:**

| Stage | Dimension/s | Strategic goal/s |
|---|---|---|
| First Stage: Enhancing the performance of internal services and interlinking computerized systems. | Systems and software<br><br>Technological infrastructure | Enhancing digital infrastructure and technological tools. |
| Second Stage: Building capacities and enhancing the management of change and resilience to guarantee continuity of services. | Sustainability<br><br>Trust and culture | Building capacities and enhancing the management of change<br><br>Enhancing culture and digital society |
| Third Stage: Enhancing external e-services and enhancing citizen digital tools. | E-services | Enhancing digital infrastructure and technological tools |
| Fourth Stage: Enhancing community's culture in order to realize a resilient digital society | Sustainability<br><br>Trust and culture | Building capacities and enhancing the management of change |

| | | |
|---|---|---|
| | | Enhancing culture and digital Society<br><br>Enhancing digital resilience |

**Table of indicators for measuring the realization of the strategy:**

| Strategic Goal | Performance indicator/standard | Period |
|---|---|---|
| **Enhancing the service of the local government sector (First Stage)** | Enhanced services, their procedures and details are annually updated in the procedural manual adopted by the municipal council. | Within the first two years |
| | Availability of an effective online archive center for services provided and attachments. | |
| | The degree of improvements in the speed of service delivery adopted by the municipal council exceeds 20%. | |
| | Number of finalized service requests accomplished at the municipality within the dedicated time mounts to over 60%. | |
| | Number of requests pending at the municipality does not exceed 10%. | |
| | A public services center system that works according to the procedures of the municipality's service manual. | |
| | Availability of an effective complaints system with clear classification of complaints. | |
| | Unifying the information of taxpayers' file. | |
| **Enhancing digital infrastructure and technological tools (Second Stage).** | Availability of municipal technological budget under the approved budget of LGUs, supported by the decisions and activities adopted by the local authority council that supports transforming into a digital municipality. | |
| | Availability of action plans with identified responsibilities and timeframe for implementing each plan and the methodology for implementation monitoring and evaluation based on the budget. | |
| | Percentage of technological and information infrastructure readiness of LGUs for transforming into digitalized municipalities is approximately 70%. | |
| | Annual technological assessment and identifying the technical needs in line with the municipal technological budget. | |
| | Percentage of technical information accuracy of LGUs with regards to transforming into digitalized municipalities exceeds 80%. | |

| | | |
|---|---|---|
| | Availability of computerized systems linked to the municipality's basic systems (services center, financial system, complaints system, and archiving system). | |
| | Availability of protection licenses and applying IT policies in LGUs. | |
| **Building capacities and enhancing the management of change (Third Stage)** | Training courses for those working in the field of digital management, services and tools. | Within three years. |
| | Number of policies/ procedures/ guidelines that motivate LGUs and citizens to use e-services. | |
| | Number of legislations/ laws/ codes and regulations supporting digitalization services. | |
| | Percentage of increase in active e-accounts out of the total number of taxpayers. | |
| | Percentage of increase in e-transactions executed annually out of the total number of transactions. | |
| **Enhancing culture and digital society (Fourth Stage)** | Meetings and public polls. | Within 4 years. |
| | Publishing citizen budget to achieve transparency. | |
| | Digital awareness activities targeting the public. | |
| | Specialized administrative workshops or training courses for employees. | |
| | Training courses for those working in information and communication technology on the optimal use of modern technology. | |
| **Enhancing digital resilience (Fourth Stage)** | Availability of a resilience plan that includes information and digital resilience. | |
| | Number of coordination mechanisms applied in projects that enhance resilience. | |
| | Percentage of resilience plan implementation by LGUs. | |

## Monitoring and Evaluation:

1. Implementing the strategy is mainly the responsibility of LGUs in collaboration with relevant partners.
2. Monitoring the implementation of the strategy shall be mainly the responsibility of MoLG.
3. A committee for monitoring the implementation of the strategy shall be formed, to be chaired by MoLG, with the participation of MDLF and APLA as members, as well as any other party the Ministry deems fit.
4. The tasks of the strategy implementation monitoring committee shall be as follows:
    1) The committee conducts periodic meetings, once every three months.
    2) Developing the required forms and tools for monitoring the realization of strategic goals and the implementation according to performance indicators, which can be reviewed and improved according to the strategic developments and following a piloting process.
    3) Conducting periodic assessment processes on the reality of LGUs concerning digitalization. The committee shall use the help of consultants to conduct assessment processes as needed, guaranteeing transparency by publishing the assessment results.
    4) Developing proposals for the development of new programs and projects to help achieve the strategic goals, and participating in the follow up of ongoing programs and enhancing their consistency with the strategy.
    5) Preparing and submitting annual and periodic reports to H.E. Minister of Local Government, which should at least include the results of assessing the reality of LGUs, challenges, lessons learned and recommendations.

# Annex No. (1): Analysis of current reality of the local government sector in the area of digital transformation

## Analysis of LGUs current reality:

*(1)* ***A survey to assess the reality of IT in LGUs***

This survey was divided into seven parts to understand the general situation in relation to digitalization in LGUs as follows:

First part: General information.

Second part: Digital infrastructure and computerized systems.

Third part: Digital services.

Fourth part: Data privacy and information security.

Fifth part: Planning, development and IT cadres.

Sixth part: Cooperation and participation.

Seventh part: Training and performance appraisal.

**The following shows the details of the questionnaires and its different parts:**

**IT reality in LGUs' assessment questionnaire**

**First part: General Information:**

| | |
|---|---|
| Name of local authority | |
| Number residents in the local authority | |
| Number of employees in the local authority | |
| Governorate | |
| Classification of local authority | **Circle the right answer: (Municipality A, Municipality B, Municipality C, Village Council) |
| Number of IT employees in the local authority | |
| Contact information of the respondent | Name: |
| | Job title: |
| | Mobile number: |
| Date of completing questionnaire | |

**Second part: Digital infrastructure and computerized systems:**

| | Statement | Not available | Poor | Intermediate | Good |
|---|---|---|---|---|---|
| 2.1 | Availability of a computer network and its accessories (firewall, switches, virtual networks, guidance devices) in the local authority. | | | | |
| 2.2 | Availability of a room dedicated for servers and managing communication networks. | | | | |
| 2.3 | Availability of computer devices and its accessories. | | | | |
| 2.4 | Availability of internet service | | | | |
| 2.5 | Availability of backups and data retrieval – within the local authority premises. | | | | |
| 2.6 | Availability of backups and data retrieval – outside the local authority premises. | | | | |
| 2.7 | Total storage capacity. | | | | |
| 2.8 | Availability of cloud services. | | | | |
| 2.9 | The local authority has a center for recovering from disasters. | | | | |
| 2.10 | The degree of automation of internal work procedures. | | | | |
| 2.11 | Availability and use of Geographical Information Systems (GIS). | | | | |

**Third part: Digital services:**

| | Statement | Not available | Poor | Intermediate | Good |
|---|---|---|---|---|---|
| 3.1 | Availability of an official website for the local authority. | | | | |
| 3.2 | Availability of applications (web/ mobile) for citizens to access local authority information. | | | | |
| 3.3 | Availability of applications (web/ mobile) for citizens to access services provided by the local authority. | | | | |
| 3.4 | Availability of e-services for paying bills, such as electricity and water. | | | | |
| 3.5 | Availability of e-services for transactions conducted at the LGUs, such as applications for licenses. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 3.6 | The degree of taking into consideration building e-services for persons with disabilities. | | | | |
| 3.7 | The degree of citizen participation in designing and creating e-services. | | | | |

**Fourth part: Data privacy and information security:**

| | Statement | Not available | Poor | Intermediate | Good |
|---|---|---|---|---|---|
| 4.1 | Availability of security measures for protecting the data of local authority and citizens. | | | | |
| 4.2 | The degree of applying information security policies to electronic systems of the local authority. | | | | |
| 4.3 | Applying data retrieval policies and making sure data is not misplaced. | | | | |
| 4.5 | Applying data privacy measures to citizens' data at the local authority. | | | | |
| 4.6 | The degree of conducting security assessments by external parties. | | | | |

**Fifth part: IT planning, development and cadres:**

| | Statement | Not available | Poor | Intermediate | Good |
|---|---|---|---|---|---|
| 5.1 | Availability of strategies for transforming LGUs into a digital system**.** | | | | |
| 5.2 | Availability of a plan for enhancing digital infrastructure and digital transformation. | | | | |
| 5.3 | Availability of a dedicated budget sufficient for supporting digital transformation at the local authority. | | | | |
| 5.4 | Citizen participation in developing digital transformation strategies for LGUs. | | | | |
| 5.5 | The degree of sufficient IT cadre at the local authority – in terms of number. | | | | |
| 5.6 | The degree of sufficient IT cadre at the local authority – in terms of capacities and required experiences and expertise. | | | | |
| 5.7 | Availability of a cadre specialized in developing web and mobile applications. | | | | |
| 5.8 | Availability of a person specialized in information security. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 5.9 | Availability of a person specialized in the field of geographical information systems (GIS). | | | | |

**Sixth part: Cooperation and participation:**

| | Statement | Not available | Poor | Intermediate | Good |
|---|---|---|---|---|---|
| 6.1 | Cooperation and contracts with the private sector to capitalize on the experiences in digital transformation for the local authority. | | | | |
| 6.2 | Cooperation with academic institutions to capitalize on the experiences in digital transformation for the local authority. | | | | |
| 6.3 | Partnerships with local community organizations to enhance digital transformation. | | | | |
| 6.4 | Partnerships with regional or international organizations in the field of digital transformation. | | | | |

**Seventh part: Training and performance appraisal:**

| | Statement | Not available | Poor | Intermediate | Good |
|---|---|---|---|---|---|
| 7.1 | Availability of training and digital awareness programs for employees to enhance their digital skills. | | | | |
| 7.2 | Availability of training and awareness campaigns for citizens to increase their technical and digital awareness. | | | | |
| 7.3 | Availability of periodic assessments to test the readiness for digital transformation and to measure the progress of LGUs in that regard. | | | | |
| 7.4 | Availability of periodic assessments to test citizens' acceptance of and satisfaction with provided e-services. | | | | |
| 7.5 | Availability of analysis of the results of periodic assessments, training and awareness programs. | | | | |

**Eighth part: Obstacles and challenges:**

**Open questions: Please go ahead and answer the following questions:**

**First question:** What are the main obstacles and challenges facing LGUs in achieving digital transformation?

---
---
---
---

**Second question:** What are the suggestions to enhance the level of digital transformation at LGUs?

---
---
---
---

*(2)* ***Methodology:***

The survey questionnaire was published using google forms, with a deadline for completion on August 31, 2023. In return, the Team made follow ups to increase the number of responses via phone calls and emails. The total number of responses received by the deadline was (86) eighty six.

It was agreed to follow a compiling mechanism for the questionnaires for analysis purposes to be as follows: (Municipality A, Municipality B, Municipality C, Village Council).

Data received from the questionnaires was summarized and processed, as questions were encrypted with distinct identifiers using open data standards. Moreover, special attention was given to the privacy of data by removing any personal information, particularly contact data and information.

Likert Scale of four points was applied to transform data from qualitative to quantitative to facilitate the process of elaboration and statistical analysis. An evaluation system was adopted that uses a points scale that starts with 1 and finishes with four; 1 being nothing or not available, 2 poor, 3 intermediate and 4 good. Some of the answers gave more than one evaluation point, therefore the lowest was considered for study accuracy purposes.

The variables for population numbers and number of LGUs' employees were specially processed by following a statistical period style, with the aim of facilitating the statistical analysis process and to allow the tabular report processor to recognize the links and crosscuttings between data.

Moreover, data from parts 2-7 were compiled into specific themes to facilitate the analysis process according to the governorates and local authority classification.

*(3)* ***General results:***

A. Part two: Digital infrastructure and computerized systems

Digital infrastructure, computerized systems and their associated IT tools are available, in addition to internal digital services and in-house hosting of systems. The study showed that 55.8% of LGUs has an intermediate level of digital infrastructure and computerized systems. The study also showed that 44% of LGUs have internet services and in-house hosting of systems. Furthermore, the study shows lack of centers for recovery from disasters.

B. Third part: Digital services

The study showed that 79% of LGUs lack digital services or do have digital services but are very poor, and it also showed that 15% of LGUs have digital services that are intermediate.

Concerning websites, the study showed that 44% of LGUs have official websites, and it also showed that 15% of LGUs do not have any official websites.

C. Fourth part: Data privacy and information security

The study showed that 47.7% of LGUs consider and are interested in maintaining the privacy of data and has information security systems, whereas 37.2% do not have such systems, or have them but in a primitive form.

Concerning risk assessment, the survey showed that 50% of LGUs did not conduct any form of risk assessment using a third party.

D. Fifth part: Planning, Development and IT cadres

The field of IT planning, development and cadres suffers a 58.1% shortage for several reasons, most importantly, the lack of allocating required budgets. There is also a shortage in citizens' participation in most of the LGUs in relation to the development of digital transformation strategies. Only 37.2% of these LGUs have active strategies, allocated budget and cadres in the field of IT.

E. Sixth part: Cooperation and participation

It appears that there is a deficiency in cooperation in the area of quadripartite innovation (private sector, academia, and local communities, regional and international organizations), which may hinder the implementation of the national digital strategy at the level of local government. The survey indicates that 42% of LGUs do not have any form of cooperation with the private sector and 22% have limited cooperation. There is no cooperation with the academic sector (81%), and no cooperation with the local communities (83%), whereas lack of cooperation between LGUs, regional and international organizations reached 86%.

F. Seventh part: Training and performance appraisal.

The survey showed that 86% of LGUs do not have any mechanisms for training and performance appraisal. The study indicates that 54.7% of LGUs do not have any mechanisms and 31.4% have mechanisms that are classified as very poor.

The study also showed that only 2.3% of LGUs have effective mechanisms for training and performance appraisal.

### *(4) **Relationships between the different variables***

Relationships between the different variables were analyzed with the aim of acquiring further observations and results; general information variables related to the governorates, LGUs' classification and number of employees as well as the state of digitalization were all processed using crosstab, linking them and analyzing them according to the six fields of the study, as follows:

A. Governorates:

LGUs in Gaza Strip exceeded their counterparts in the west bank in all six fields; Ramallah and Khan Younis governorates reached an advanced level due to owning effective systems in all six fields. On another hand, all governorates indicated some LGUs that do not have e-services, and many indicated systems for protection of data privacy and information security working at an intermediate level. In another context, there is a shortage in IT, planning and development cadres in half of the governorates, in addition to lack of cooperation and participation, absence or weakness in terms of specialized systems for training and performance appraisal in all governorates.

B. Classification of LGUs and number of employees:

Regarding the classifications and number of employees, the study shows that local village councils comprise of at least ten employees. In the municipalities located in Area C, number of employees varied between 10 and 49 in 29 LGUs, two of which mentioned having 400 or 500 employees, both in Gaza Strip, with a population ranging between 230,000 and 470,879 each. As for municipalities located in Area B, they had a large number of employees starting from 10 employees and mounting up to over 1000. Most of them had between 25 and 49 employees, and two municipalities located in Area A with 50-74 employees; however, the rest had a total number exceeding one hundred employees.

C. Classification of LGUs and the status of digitalization:

Most LGUs, regardless of their classification, show availability of current digital foundations of intermediate quality. E-services however appeared to be nonexistent or poor in all departments, and municipalities in Area C suffer a high shortage in such services, despite the availability of good data privacy and information security measures. As for planning, development and IT cadres,

they either suffer weaknesses or are available at an intermediate quality in all sixty three municipalities of all four classifications. Finally, it was evident that cooperation, participation, training and performance appraisal in all LGUs are poor or nonexistent at all.

D. Number of employees and status of digitalization:

Regardless of their size, most LGUs appear to have a basic infrastructure for digitalization. However, e-services appear to be poor or nonexistent in all size-classifications except those with over 1000 employees. All LGUs have good data privacy and information security except those with employees between 10 and 24. There are only three groups of good cadres in planning, development and IT, showing a good level of cooperation and participation. However, the rest suffer weak or absent cooperation and participation. All groups confirmed having weak or absent programs for training and performance appraisal.

## (5) Implications and impact of the results of the analysis of LGUs on the digitalization strategy in the local government sector

Despite the availability of good computerized systems and accessories, as well as good internet connectivity at LGUs, there is a shortage in the necessary foundations such as data centers and centers for data retrieval in order to be consistent with the e-services provided to citizens, and enhance LGUs' work. Therefore, it is preferable to establish these data centers and capitalize on existing centers as an auxiliary alternative or centers for data retrieval. E-services are poor or lacking in all classifications, given that providing them to citizens must be smooth, undisrupted, and immediately available. Moreover, these services should be connected to the centralized government in order to facilitate access and handling, which must be part of the basic structure of the annual plans of LGUs.

Furthermore, the survey showed that 63 municipalities suffer weakness in planning, development and IT cadres in all of their four classifications, therefore, the issue must be seriously considered in the annual plans to fast track the digitalization process in all LGUs. Mechanisms of participation, cooperation, and training as well as performance appraisal systems in all classifications of LGUs also appeared weak. This calls for a serious commitment from MoLG, MDLF and ALA to each play their role in facing these issues and fostering the digital transformation project as part of systematic planning and work towards smoothly providing e-services to citizens and LGUs' employees.

**SWOT analysis of the IT reality in LGUs:**

| Strengths | Weaknesses |
|---|---|
| Intermediate digital infrastructure: availability of digital infrastructure and computerized systems in more than half of LGUs reflects their readiness to benefit from digital technology in enhancing performance and improving services. | Lack of e-services: the majority of LGUs lack the provision of effective e-services, which hinders their ability to meet citizen needs effectively and obstructs the enhancement of engagement between local governments and the community. |
| Information security and data protection systems: availability of information security systems at an acceptable level in most of the LGUs, especially municipalities, shows interest in protecting data and sensitive information, which creates great trust among the citizens and beneficiaries of governmental services. | Lack of planning, development and IT cadres: lack of qualified cadres in this field hinders LGUs' ability to develop and improve digital infrastructure and the provision of better services. |
| Availability of official websites for LGUs: availability of official websites for some LGUs represents an opportunity for enhancing communication with citizens and provision of services in a better and more inclusive manner. | Poor cooperation in the area of innovation associated with digital transformation with the private sector, academia, local communities and regional organizations. |
| | Lack of centers for recovering from disasters. |
| | Insufficient risk assessment: may lead to exposing LGUs to potential threats to the continuity and quality of its work. |
| | Limited training programs and awareness campaigns in the field of digitalization. |
| **Opportunities** | **Threats** |
| Governmental interest at the national level in the field of digital transformation and working on meeting the requirements of transformation from the legal, administrative, financial and technical aspects. | Financial challenges and limited budgets: may limit the ability to invest in the improvement of digital infrastructure and providing complete and inclusive e-services. |
| The accelerating advancement and development in IT, which provides an opportunity for providing high quality digital services. | Exposure to cyber attacks in light of lack of sufficient security procedures (security assessments by external parties, centers for recovering from disasters). |
| Enhancing collaboration with the private sector, academia, local communities and regional organizations: an opportunity for exchanging knowledge and experiences, and jointly developing technological solutions, | Lack of security and political stability. |

| | |
|---|---|
| which contributes to enhancing capacities and developing services. | |

Therefore, LGUs must adopt comprehensive and inclusive strategies that build upon the strengths and work on improving weaknesses and benefiting from available opportunities, meanwhile taking measures for facing potential threats.

## Assessing the reality of IT in each of the following:

## (Ministry of Local Government (MoLG), the Municipal Development and Lending Fund (MDLF), and the Association of Palestinian Local Authorities (APLA))

**Questions approved as the basis for the assessment of the institutions affiliated with LGUs:**

**IT infrastructure:**

1. What type of infrastructure is used in the institution (local, cloud, hybrid)?
2. What is the main purpose of each server (email server, databases, web server)?
3. Specifications of devices for each server, such as memory and the processor.
4. The operating system on each server
5. Are servers in one location or distributed to different locations?
6. Are clustering or load balancing technologies used on the servers?
7. What safety procedures are applied at the level of servers such as protection systems against attacks and firewalls?
8. Is there a policy for replacing old servers with the most advanced technologies?
9. Are virtual systems used, such as virtual servers? Kindly provide details on its use and management.
10. What are the technologies used to guarantee sustainability and availability of infrastructure.
11. Are network devices (such as firewalls, routers and protection walls) used? What are they comprised of?

**Network and communications:**

1. Kindly describe the network used in the institution (wired or wireless) and type of technology used (Ethernet cat 5 or 6, Wi-Fi or Wi-Fi 6).
2. Kindly describe the network topology (star network, ring network or tree network).
3. Is load balancing technology used for enhancing the network performance?
4. Are aggregation switches systems used to link sub networks?
5. What are the technologies used to secure the network against cyber attacks and data breaches?
6. Are intrusion detection systems used to monitor and detect unwanted activities on the network?
7. How are communications with external networks secured and monitored?
8. Are DHCP or IP servers used, and how is the distribution of addresses managed?
9. How can remote connection be done safely? Are special VPNs used?
10. How is the network managed and monitored? Are special tools used for monitoring the network performance and maintenance?

**Information security:**

1. What security measures are taken to protect the institution's data and other information?
2. What kind of security threats are the institution and data exposed to, such as cyber attacks or leaks?
3. Does the institution use intrusion detection systems to detect unauthorized activities?
4. How are security activities monitored and how is the integrity of systems regularly verified?
5. Do you have emergency plans for handling the disruption of services or cyber attacks?
6. How do you guarantee data retrieval and resuming business quickly in case of a security defect or disruption of services?
7. Do you use coding systems for data transfer and storage?
8. How are access permissions to institution's data and resources managed?
9. Is the principle of the "minimal privilege" applied to employees?
10. How do you enhance security awareness among employees and users? Do you provide training courses on information security and secure online behavior?

**Data management:**

1. What type of data do you handle at your institution?
2. How is data stored and managed in the institution? Do you use database systems?
3. How is data stored in the institution? Do you used local or cloud storage systems?
4. Do you use certain models for data storing and organization, such as the relationships model or document model?
5. What are the structures and arrangements you use to organize data within databases?
6. How do you guarantee the quality of data? Do you use procedures for verifying the accuracy and completeness of stored data?
7. Do you compile data from different sources (such as external applications or data from sub-branches)?
8. How do you deal with data safety? Are there procedures for providing access permissions to data based on the user's role?
9. What are the applied procedures for protecting sensitive data against unauthorized access?
10. What data backup procedures do you use to guarantee availability of data in case of any defect?
11. Are there periodic tests on data retrieval from backups to confirm the efficiency of retrieval processes?
12. In case of storing backups outside the institution, where is this data stored (State, City)?
13. What management systems for backups are used in the institution?
14. What technology is used for making data backups?
15. What is the mechanism of backups (manual, automatic) and the period between data backups?

**Management of services and maintenance:**

1. How is hardware and software managed and maintained in the institution? Do you use service management systems?
2. How are potential malfunctions and issues of systems and infrastructure monitored and documented?
3. Do you have periodic maintenance plans for hardware and software?
4. How are software updating and upgrading processes managed?
5. What it is the policy applied for security updates?
6. Are there periodic updating procedures for software and data security applications?

**IT teams:**

1. How many IT staff members are there in the institution? What specializations and functions is the team comprised of?
2. How is IT work planned and coordinated to guarantee the effective provision of support and services?
3. How are tasks distributed and how are priorities managed?
4. Do you use project management tools to monitor and coordinate the team's work and activities?
5. Do you develop the skills of the team members?
6. What kind of efforts are made for keeping up with technological developments?
7. How does the team deal with technological crises?

a) **Analyzing current reality of MoLG:**

**Observations and summery of answers:**

**IT infrastructure:**

1. IT infrastructure at MoLG relies mainly on servers located at the Ministry, where several servers exist such as (e-archive system server, personnel affairs system, and the budget portal system). All these servers are fully hosted at the Ministry; meanwhile other system servers are used at the governmental computer center affiliated with the Ministry of Communication and Digital Economy (MTDE).
2. The Ministry uses Blade servers, which resources are divided using (VMware), and uses (Windows Sever 2018, Windows Server 2016 & Linux) operating systems, except for the Geo-MOLG system server located on the governmental computer servers at the Ministry of Communications and Digital Economy.
3. The servers inside the Ministry use a clustering system and load balancing system at various degrees on each server or (VM).
4. The servers at the Ministry are protected through safety gates using passwords, which are only available to a limited number of IT employees only at the Ministry. As for the data on these servers, it is protected using (Fortinet Gate Firewall) and Endpoint Antivirus system.

5. Concerning hardware or infrastructure replacement policies, they exist; however, the extent of its implementation is linked to the financial factor and its availability to the Ministry.
6. A VEEM system is used to create virtual systems and servers, and includes many features and tools for guaranteeing sustainability of data. Servers are linked through (V-Lan) to guarantee data exchange and quality of transfer among them.

**Network and communications:**

1. The Ministry uses a wired internet network using CAT7 cables and another wireless network using (Wi-Fi 6) system. Both networks are subject to the same rules to guarantee the safe transfer of data without interruption in terms of the quality of associated hardware. Both networks use load balancing, as each floor at the Ministry has a distribution network linked to the main one. Concerning the Directorates, each Directorate has its own network and an address system different from the main network, but is linked through the server in each directorate. Through sub-networks and the main network, aggregation switches are used to link them together in order to guarantee sending and receiving data. Floor switches and core switches are used at the Ministry.
2. The network is secured by using Fortinet Gate Firewall and Endpoint Antivirus to guarantee no intrusion or leaking of data. External communications with the directorates or the governmental computer are monitored using (VPN), and the Ministry lacks intrusion detection systems.
3. IPs are distributed through a DHCP server by using (V-Lans), providing addresses to each new device based on the distribution of floors and through this technique old and new IP addresses are managed.

**Information Security:**

1. Data available on servers is protected, especially that these servers exist in the Ministry in one of two ways, the first in the form of protection systems and surveillance cameras to prevent direct access to this data. As for online access, it is protected by a firewall and an antivirus, and further protection is needed by making local backups of data.
2. The highest risk it is exposed to is the denial of service (DoS), however, despite this threat; the Ministry uses basic tools rather than advanced ones to prevent these threats and it does not use intrusion detection systems for protecting its data. Proper functioning of safety systems is monitored through acquiring updates of the operating systems and antivirus knowing that the Ministry has no emergency plans for dealing with disruption of services or cyber attacks.
3. In case of any issues related to data, data is retrieved using local backups, as for the data stored on e-clouds, they are also considered local, as it is located in the governmental computer, which is located in the same geographical area. Moreover, the Ministry does not encrypt the data on the cloud by itself, but rather it relies on the governmental computer for the process of data encryption.
4. Users' access to available data on the systems is managed using a user authentication login, as well as users' permissions to access files through a firewall (users rule).
5. There are no technical courses or workshops for employees to enhance data security awareness or knowledge on the cyber attacks the Ministry might be potentially exposed to and means of prevention, or courses on secure behaviour in relation to information.

**Data management:**

1. The Ministry uses almost all types of data (written data, geographical data, visual and audio files). Such data is stored depending on the relevant system, for example, geographical data is stored through (Geo-MOLG) system and employees' data through the HR system, and e-archiving system. All these systems use data management systems (MySQL, Oracle) except for the management of employee files, which does not use any particular system but rather uses a files system for organizing data, similar to the way an operating system (Windows) works, while making data backups locally and on the cloud.
2. Quality of data is verified using data management systems (MySQL) to guarantee the quality of data and its consistency with the data available at the Ministry and completing making backups of this data. Moreover, some data from external sources is merged, such as the data of LGUs' budgets. Furthermore, users' access to this data happens at the level of the system and firewall (user rules).
3. Backups are made in an automatic and scheduled manner, were these copies are locally stored (within the Ministry) or on the e-cloud (governmental computer). Data is periodically checked to guarantee its safety from any harmful files, in addition to testing the retrieval of such data periodically to guarantee its quick and proper retrieval. The Ministry uses VEEM system for managing the processes of data backups and retrieval.

**Management of services and maintenance:**

1. Manual management and maintenance of hardware and software, and documentation of malfunctions.
2. Plans for conducting periodic maintenance of hardware and updating systems are available, however, these plans usually are not made periodically, rather, they are developed when issues emerge, in most of the cases. Software updating processes are done per need, whereas the updating or development of infrastructure is done in case of availability of the financial factor necessary for its implementation.
3. Specific policies for updating hardware and software or conducting periodic updates are lacking, update and upgrade processes are activated per need only.

**IT Teams:**

1. There are 7 IT employees at the Ministry with no IT personnel in the Directorates, therefore the IT staff at the Ministry operates from the Ministry's HQ and the Directorates simultaneously.
2. Inside the Ministry there are two main departments specialized in IT who work in close coordination with one another in case of malfunctions, software updates, infrastructure, and balancing loads. Loads are balanced among IT employees based on their specializations, and there is no system for project management to help monitor, coordinate and distribute tasks among employees.
3. There are no specialized training courses for IT employees. Developing technological capacities happens through individual efforts without any plans for conducting specialized training courses in IT at the Ministry.

**SWOT Analysis:**

| Strengths | Weaknesses |
|---|---|
| 1. Availability of servers and infrastructure inside the Ministry allows for full control over systems and data, which increases safety and control.<br>2. Using modern technologies: using Blade servers and VMware allows the effective and efficient division of resources.<br>3. Using firewalls, anti-virus software and data protection systems contributes to enhancing data security.<br>4. Load balancing and clustering of data: using on-server clustering techniques and load balancing guarantees the sustainability and efficiency of systems.<br>5. Data types: the ability to use and manage a wide range of data types enhances flexibility of the Ministry in processing information.<br>6. Data management systems: using data management systems helps guarantee the quality of data and its effective organization.<br>7. Backup processes: conducting periodic backup and data retrieval processes contributes to achieving data sustainability and guaranteeing the prevention of its loss. | 1. Lack of security awareness: lack of training courses or workshops to enhance security awareness among employees may leave the Ministry vulnerable to security threats.<br>2. Lack of intrusion detection systems: lack of intrusion detection systems may leave the Ministry vulnerable to undetected attacks.<br>3. Lack of emergency plans: lack of emergency plans for facing disruption of services or cyber attacks may increase its adverse impact.<br>4. Management of manual maintenance: reliance on manual management and maintenance of hardware and software may not be effective and may increase the chances of human error.<br>5. Lack of a specific policy for updates: lack of specific policies for the updating and maintenance processes may lead to delays in improving infrastructure. |
| **Opportunities** | **Threats** |
| 1. Enhancing security awareness: the possibility of providing training courses and workshops to employees to enhance their security awareness and skills in the area of information security.<br>2. Developing intrusion detection systems: the possibility of enhancing the safety structure through implementing intrusion detection systems for monitoring cyber attacks and responding to them.<br>3. Using intrusion detection software such as Cisco NGIPS and Fidelis Network. | 1. DDoS attacks: attacks that may adversely affect the stability of services and require the development of strategies for its prevention and effective response.<br>2. Lack of emergency planning: lack of emergency plans may leave the Ministry vulnerable to malfunctions and loss of date in case of crises.<br>3. Insufficient safety: lack of using advanced safety systems may cause infrastructure to be vulnerable to advanced security threats, such as using the WAF system. |

| | |
|---|---|
| 4. Using intrusion detection hardware such as FireEye Intrusion Prevention System and Hillstone S-series.<br>5. Storing data on the cloud: increasing the use of cloud storage along with data encryption may enhance securing data and responding to the changing needs.<br>6. Enhancing maintenance and updates: the possibility of organizing maintenance and update processes to enhance infrastructure performance.<br>7. Organizing processes: the opportunity to organize and guide the management of processes through appropriate system applications.<br>8. Development of capacities: providing training courses to IT employees may help develop their skills and increase their awareness in information security.<br>9. Benefiting from services provided by the Ministry of Communications and Digital Economy (MTDE) pursuant to the Council of Ministers Decree No. 06/151/18 of 2022. | 4. Margin of human error: relying on manual management allows opportunity for human error and delays in maintenance and updates.<br>5. Loss of data: lack of specific policies for updates may increase the risk of data loss.<br>6. Insufficient offline backup in terms of best practices, systems and equipment that can be used for conducting data retrieval.<br>7. Lack of coordination: lack of IT employees in most of the Directorates affiliated with the Ministry may affect the coordination among the team members and effective distribution of tasks. |

**Recommendations:**

1. To implement advanced DoS protection systems.
2. To develop response plans for DDoS attacks including early detection and quarantining of suspicious activities.
3. To develop and implement comprehensive emergency plans including data retrieval and providing clear guidance for teams in cases of crises.
4. To organize periodic trainings for the teams based on the emergency plans.
5. To assess technology infrastructure and update the safety systems in accordance with the most recent best practices.
6. To enhance awareness on information security among employees, and to develop safe usage policies for systems and software.
7. To adopt automated management systems for maintenance and update in order to reduce human error.
8. To provide continuous training to employees on maintenance and safety tasks.
9. To develop periodic policies for backup and data retrieval processes.
10. To implement encryption solutions and controlled access, in order to protect data against unauthorized access.
11. To implement advanced systems for detecting intrusion to monitor unauthorized access within the infrastructure.

12. To develop emergency plans including immediate response to disruption of services or cyber attacks, and quickly regain security and safety.
13. To adopt automated management systems for the maintenance of hardware and software in order to enhance efficiency and reduce human error.
14. To develop policies and timeframes specifically for the updates and maintenance processes, and to regularly implement them.

## b) Analysis of current reality of the Association of Palestinian Local Authorities (APLA):

**Observations and summery of answers:**

Following the visit of APLA's office, answers to each section of questions were as follows:

### IT Infrastructure:

1. APLA mainly relies on an e-archiving system server for storing and archiving data, a server for the management, monitoring and control of the internal network, VMware for dividing available resources, and an operating system (such as Windows Server 2019). Moreover, it uses cloud storage only for APLA's data backups.
2. All servers are located in one place inside APLA's office and the servers are directly protected through a fingerprint access only granted to APLA's Executive Direct and IT employee. Furthermore, there are security cameras for monitoring the existing servers, and APLA provides insurance for these servers.
3. APLA does not use clustering and load balancing techniques for existing servers due to lack of pressure on data sent or received by APLA.
4. There are no policies for replacing or updating existing servers, however updates occur depending on work needs, and recommendations are provided through APLA's IT employee.

### Network and communications:

1. Availability of two networks within APLA, one used only for computers and the other is used for smart phones or other devices, which is separated from the main network. It uses a (Cat6a) wired network and a wireless network.
2. Concerning load-balancing processes, none of these systems exists, due to the low pressure on the network and servers of APLA. As for data aggregation switches and clustering of data from both networks, it does not exist as both mentioned networks are not directly connected.
3. APLA uses FortiGate Firewall, for protecting the network from cyber attacks, and the email server protection is embedded in the operating system. The network is monitored and the officials are informed of any attack or unauthorized access to the network.
4. APLA uses special VPN lines for communication processes outside of APLA, especially with regards to data stored on the cloud.

**Information security:**

1. In case of any process or attempt of intrusion on the network, the network goes into complete shutdown. APLA was never exposed to threats before at the level of the office, and it uses intrusion detection systems. APLA's IT employee tests the network and data twice a week.
2. Regarding APLA's emergency plans, there is a backup server and there is an agreement with an external provider to provide data in cases of loss or corruption. As for the data stored on the cloud, there is an agreement with the company providing cloud services to APLA to encrypt data and store it in a proper location, monitoring it and avoiding any cyber attacks against or leaking of such data.
3. There is a system of permissions used for employees to access information, which are granted in line with their position and relevance to such data. Permissions are granted based on a policy agreed upon by APLA's President and the IT employee. Through the permissions system a minimal privilege approach is applied to guarantee information security from leakage or unauthorized access.
4. Security awareness of employees and its importance is enhanced through periodic courses targeting the employees to keep them informed of the latest updates on means of protecting data.

**Data management:**

1. APLA deals with several types of data (video files, text files) and other types. Such data is stored internally and externally (cloud storing) and part of this data is stored using MySQL and Oracle systems. However, the largest portion of data is stored through a file system, through which data is classified into folders or files existing on the servers, in addition to making backups on the e-cloud.
2. With regards to quality of data, APLA does not receive data unless through official authorities and only after verifying data before conveying it to the employees through a firewall and an antivirus software.
3. Data is only accessible through certain permissions granted in advance to employees in order to guarantee the prevention of leakage or unauthorized access.
4. In terms of data backup processes at APLA, they are done automatically (weekly and daily), whereas, for data stored on the cloud, the provider is the one responsible making backups of this data , as the data is stored in a location in Ramallah and another inaccurately identified location (in Czech or the United States).
5. Data verification, matching and integrity are periodically tested by taking part of the backups, comparing and checking its quality.
6. Concerning the data stored at APLA, VEEM systems are used for making backups automatically and simultaneously.

**Services and maintenance:**

1. There are no systems for managing the maintenance and software update. Such task is carried out by a part time IT employee, and for the data stored on the cloud, the company providing cloud services is responsible for carrying out that task.

2. APLA uses a manual mechanism for documenting malfunctions and hardware maintenance.
3. APLA has plans for the process of servers' updates and upgrades, which are developed annually.

**IT teams:**

1. No fulltime IT employee is available at APLA, but a part time one is.

**SWOT Analysis:**

| Strengths | Weaknesses |
|---|---|
| 1. Cloud storage: relying on cloud storage provides APLA with flexibility and the ability to expand storage capacity quickly and efficiently.<br>2. Applying strict permissions to access data decreases the risk of leakage and unauthorized access.<br>3. Using effective means of protection at APLA such as server access permissions.<br>4. Strict use of permissions on employees' access to data.<br>5. Effective use of internal and external data backups.<br>6. Effective and periodic network monitoring processes.<br>7. Monitoring the quality of data and verifying its integrity.<br>8. Periodic testing of backups.<br>9. Periodic courses to increase awareness on information security among employees.<br>10. Using a hybrid system for services and data. | 1. A small number of servers at APLA's office and extensive reliance on could storage.<br>2. Intensive use of the file system for storing data with simple use of data management systems such as MySQL and Oracle.<br>3. Lack of systems for managing maintenance and software update files may lead to missing periodic maintenance and system updates.<br>4. Availability of a part time IT employee may increase delays in handling technical issues.<br>5. Lack of specific plans and policies for IT infrastructure management and continuous updates.<br>6. Lack of mechanisms for testing backups taken from the e-cloud.<br>7. Making backups of data only, without including APLA's software. |
| **Opportunities** | **Threats** |
| 1. Using intrusion detection software such as Cisco NGIPS and Fidelis Network.<br>2. Using intrusion detection hardware such as FireEye Intrusion Prevention System and Hillstone S-series.<br>3. With regards to data access permissions, they were developed through enabling data | 1. Only basic security measures are applied at the level of data access permissions without the use of advanced systems.<br>2. Relying on a part time IT employee constitutes a threat in case of any intrusion or leak. |

| | |
|---|---|
| owners to control the rights to access their data in order to make sure that all processes is authorized.<br>4. Using multi-step authentication techniques such as the 2-factor authentication (2FA) may protect data against unauthorized access.<br>5. Data flow techniques may be applied to detect unexpected changes in data over time, in case major or surprising changes were detected. | 3. Relying on the company service provider for data encryption and choosing the location of storage.<br>4. Lack of evaluation of all security procedures and policies applied and enhancing them to match the new security threats and developments.<br>5. Using a Files system instead of using data management systems completely.<br>6. Dependency on third party: extensively relying on a third party, may lead to the third party withholding provision of services, which leads to halting processes and operations.<br>7. Lack of accurate organization of update and replacement processes may leave systems vulnerable to attacks or breaches. |

**Recommendations:**

1. To enhance and expand security measures and develop access permissions in line with potential threats, as well as considering the use of advanced technologies such as multi-factor authentication.
2. To develop specific plans for periodic technological and security updates and to include the operating system and software update, and security fixes.
3. To invest in intrusion and security verification tests periodically to identify gaps and weaknesses, and to correct them before they can be exploited.
4. To hire a full time IT employee to be directly responsible for IT infrastructure, data and its security, monitoring and responding effectively to any security threats.
5. To verify the accuracy of available agreements and contracts including aspects of service provision, such as issues related to data encryption, and appropriate storage of data.
6. To conduct a periodic assessment of applied security policies and procedures and to enhance it in line with the new security threats and developments.
7. To use advanced data management systems to increase data safety and organization.
8. To implement email-tracking systems, covering all its components, to detect any potential threats before the mail reaches the employees.
9. To devise a strategy for dealing with third party providers of e-cloud services that includes the revision of safety and security requirements in existing contracts and agreements.

## c) Analyzing the current reality of the Municipal Development and Lending Fund (MDLF):

**Observations and summary of answers:**

As per the visit to MDLF, the answers to the questions prepared for each section were as follows:

**IT Infrastructure:**

1. MDLF uses a hybrid structure of servers inside its premises and on the e-cloud. All data is fully uploaded to the cloud, which is also used in cases of emergency in order to guarantee the flow of MDLF work in terms of data flow and the internal systems.
2. MDLF premises have several servers used for archiving of financial files and the website, as MDLF uses VMware for dividing servers for simultaneous multiple purposes.
3. MDLF updates the specifications of these servers according to the practical requirements, and also integrates updates according to the type of modern technology. MDLF uses Windows Server 2019 operating system as the foundation for servers, and it uses a Linux system for activating the VMware system. All servers are located at MDLF and the server room is secured to prevent the access of anyone without proper permissions, by using a secured door equipped with security measures, such as having an access pad with a passcode, completely isolated from its surroundings and equipped with two electricity lines and an additional UPS line.
4. Clustering systems are used to increase server effectiveness by pooling all servers' resources to work more effectively. Moreover, a load balancing system is used to distribute the loads to servers in case of pressure. These systems are simultaneously used with the e-cloud.
5. MDLF uses safety systems for protecting data on these servers; it uses a firewall and WAF system for isolating these servers from the outside world in order to protect them against security threats.
6. As mentioned before, servers' resources are divided and used effectively through the use of VMware, through which automatic backups are made (daily, monthly, annually) at the level of VMware and to have backups at the level of data.

**Network and communications:**

1. A Cat6a wired network, a Wi-Fi 6 wireless network, and a VOIP network are available, and each system has its own rules and limits in terms of access to information or available services.
2. It uses load balancing on the network to facilitate access to information on servers, e-cloud and MDLF employees' devices. An aggregation switches system is also used to compile data from all parts of the network; the main and sub parts.
3. The network inside MDLF is protected by using Physical Firewall IPS and a WAF system, in addition to prohibiting the direct use of USBs on devices without scanning it and guaranteeing they are free of any corrupt files. In addition, the WAF software is used as an intrusion detection system.
4. External communication with the network and employees' access to data is secured at MDLF using Microsoft Domain Authentication to identify the identity of users and access permissions to the internal network or data.

5. There are servers for distributing IP addresses (DHCP server) depending on the network connected to the device.
6. Concerning the safe remote communication, an s-VPN system is used between the West Bank and Gaza, through which a certain device will be granted permissions through a (Real IP) only and granting that IP certain permissions to access data or servers.
7. Monitoring and observing the network through an alert system activated through the antivirus admin control tools, to alert system officers in case any intrusion or cyber attack occurred.

**Information Security:**

1. MDLF uses the extended detection and response system "XDR" to detect and protect information from cyber security threats.
2. MDLF was not exposed to any significant cyber security threats, except for one cyber attack against MDLF website. The use of an intrusion detection system, Fortinet antivirus and IPS has significantly contributed to preventing cyber security threats and protecting the data available at MDLF.
3. Activities around data are always authenticated using the notifications available on the WAF system, as it identifies both, safe and other activities.
4. Lack of periodic plans, however hardware and software related to information security are updated periodically. Moreover the use of local backups (offline data backup) to guarantee availability of a local copy that can be only accessed by the IT employee, and a third party source was recruited for effective and quick data storage and retrieval.
5. MDLF data has been encrypted using a special encryption system from Microsoft, where data is encrypted as well as the means of communication itself, making access to such data difficult. In addition, concerning employees' access to data, a permissions system and a minimal privilege approach is applied to guarantee the prevention of leakage or any employee having access to certain data.
6. No courses for raising security awareness are provided to MDLF employees on safety systems or potential cyber threats and protection tools, however courses are provided on information safety for IT employees only.

**Data Management:**

1. MDLF deals with a wide scale of data types such as (financial data, website data). These files or data are managed using MySQL and Oracle systems. These systems are used within servers located at MDLF as well as on the cloud, and their data is synchronized.
2. Data quality is verified in terms of its integrity and being free of corrupt files using an automatic system (Firewall, WAF, Forty Antivirus) and also through the systems' officer at MDLF. However, data accuracy is verified in a hierarchal manner.
3. Data safety and accessibility are tackled according to the functional role of users, including the minimal privileged access, and in some cases, permissions are provided based on recommendation from the direct supervisor, where such permissions are temporary. Moreover, MDLF uses Microsoft user rules and VM systems to define access permissions to such data.

4. Automatic backups through VEEM. There is a local backup copy (offline data backup) and another copy on the cloud, given that the location of storing the backup copy available on the cloud is unidentified, and is rather managed through the company providing this service. Verifications are made to test the integrity of these data backups once every 3 months, and the speed of data retrieval is tested as well.

**Management of Services and Maintenance:**

1. Lack of specific systems for hardware management and maintenance. Management or malfunction documentation processes are conducted periodically for both, the systems and hardware.
2. MDLF has future plans for hardware and software update and maintenance at, as update processes occur through studying the increasing needs for certain services or availability of a new technology that offers further effectiveness and efficiency. Update processes are conducted based on the requirements without having certain policies for managing such updates.

**IT Teams:**

1. There is a full time IT employee at MDLF and another employee for monitoring projects related to IT infrastructure outside MDLF. Each employee does different work in terms of its nature and the responsibilities associated with it, and there are no systems for the management of infrastructure planning and development projects at MDLF.
2. Lack or scarcity of courses related to IT provided to the MDLF IT staff, as MDLF relies highly on maintenance contracts with companies that are up to date with technological advancements and also for dealing with technological crises.

**SWOT Analysis:**

| Strengths | Weaknesses |
|---|---|
| 1. Using e-clouds provides flexibility and the ability to access data anywhere at any time.<br>2. A hybrid infrastructure combining local servers and e-clouds provides flexibility and sustainability when uploading data in cases of emergency.<br>3. Using advanced operating and partition systems (VMware) increases the efficiency of servers and the utilization of resources.<br>4. Utilization of load balancing, data clustering and automatic upload of backups contributes to enhancing safety and continuity of work. | 1. Lack of targeting employees with training: lack of provision of security awareness courses to employees increases the risks of cyber attacks.<br>2. Lack of a unified standard system for hardware management and maintenance may lead to data loss or disruption of services in case of lack of good coordination.<br>3. Lack of specific policies for managing updates and their timing: MDLF is fully dependent on Microsoft only for system updates. |

| | |
|---|---|
| 5. Data encryption and applying the permissions system enhance data safety and prevent unauthorized access.<br>6. Using the extended detection and response system (XDR) for detecting security threats enhances MDLF's ability to face cyber threats.<br>7. Continuous update of infrastructure: the ability to update infrastructure and use IT increases work efficiency and data safety.<br>8. Using safety systems: using firewalls and various safety systems enhances information security and the detection of unsafe activities linked to data and internal networks. | |
| **Opportunities** | **Threats** |
| 1. Enhancing employees' guidance and training: providing employees with training in the field of information security and using systems reduces the risks of cyber attacks.<br>2. Enhancing coordination of work among IT staff helps enhance responsiveness to technological issues and problems.<br>3. Enhancing data management and coordination among IT staff may increase work efficiency and coordination between projects.<br>4. Using project management tools contributes to better hardware tracking and maintenance. | 1. Lack of specific policies for managing updates may lead to delays in applying new technologies.<br>2. MDLF relies highly on maintenance contracts with IT service providers, which exposes it to risks in case these services were not available.<br>3. Irregular updates: lack of specific policies for managing updates may cause infrastructure to be vulnerable to security gaps. |

**Recommendations:**

1. To organize periodic security awareness courses for all MDLF employees, including the updates related to information safety and proper online behavior.
2. To develop in-house awareness campaigns to highlight common safety threats and unsecure behaviour through email and other digital resources.
3. To enhance the allocation of resources: allocating more resources to provide support and necessary tools to IT staff.
4. To establish an approach and develop shared tools for project management and to document maintenance works and fixing bugs.
5. To develop and implement a standard system for hardware management and maintenance and guaranteeing its conformity with safety policies.

6. To establish specific policies for managing updates, including schedules and testing procedures.
7. To develop regular updates policy and periodic tests to guarantee the integrity of the system and applications.
8. To prepare a response plan for security threats including the procedures for handling potential attacks, to disseminate the plan to all employees and to regularly update it.

This document was accomplished in collaboration with the E-governance Program "INDIGO", funded by GIZ, mandated by the German Federal Ministry of Economic Cooperation and Development (BMZ)