Final ICT Assessment Report for Justice Institutions in Malawi

Conducted under the Chilungamo II Programme
Expert type: Non-Key Expert
Number of days:35 days
Expert name: Solomon Kwasi Andoh

Provision of Technical Assistance to the Access to Justice Programme (Chilungamo II)

Submitted on: 24th October, 2024

Final ICT Assessment Report for Justice Institutions in Malawi

Conducted under the Chilungamo II Programme

Provision of Technical Assistance to the Access to Justice Programme (Chilungamo II)

Submitted by

DT Global

In consortium with

ECORYS

This project is executed by **DT Global** and **ECORYS**

Abstract

Project Title	**Chilungamo II (Access to Justice) Programme**
Contract Title:	*Technical Assistance to the Government of Malawi in the Implementation of the Chilungamo II (Access to Justice) Programme*
Overall objective:	To improve humane and effective delivery of justice for all, especially those living in marginalized and most vulnerable situations.
Specific Objectives:	1) To strengthen democratic governance and enhance the ability of citizens, accountability institutions, and civil society to demand transparency and hold duty-bearers to account. 2) To increase access to justice for all, especially women and the poor.
Expected results:	
Key Result 1:	Improved knowledge, gender-balance skills and capacities of the key justice institutions.
Key Result 2:	Improved legal and coordination frameworks for key justice institutions.
Key Result 3:	Improved capacity of Malawi Prison Services to implement alternative sentences
Key Result 4:	Improved mechanisms and frameworks for enhanced accountability in justice institutions.
Key Result 5:	Improved physical conditions of justice system infrastructure with a gender perspective.
Key Result 6:	Improved capacity to offer legal and paralegal aid and mediation
Key Result 7:	Improved legal awareness and education among those living in the most vulnerable situations.
Duration:	48 Months
Key stakeholders:	The Government of Malawi, including the Ministry of Justice and Constitutional Affairs (MoJCA), Judiciary, Police, Prisons, Legal Aid Bureau, the Malawi Human Rights Commission, and the Ombudsman Office.

Disclaimer

This report has been produced by **Solomon Kwasi Andoh** under the framework of the Chilungamo II Programme. The contents of this document are the sole responsibility of **Solomon Kwasi Andoh** and do not necessarily reflect the views of the European Union or DT Global.

Executive Summary

1. Overview

This comprehensive ICT assessment report evaluates the current state of ICT infrastructure, data security, and staff capacity across five key justice institutions in Malawi: Malawi Legal Aid Bureau, Malawi Police Service, Malawi Human Rights Commission (MHRC), Office of the Ombudsman, and Malawi Prisons Service. The assessment is part of the Chilungamo II Programme, which aims to improve access to justice, promote human rights, and enhance institutional accountability.

2. Key Findings

The assessment revealed significant challenges in terms of outdated ICT infrastructure, limited network connectivity, weak data security protocols, and insufficient ICT skills among staff. These issues have hindered operational efficiency and the ability of institutions to deliver timely justice services. Recommendations include immediate, medium-term, and long-term actions to modernize infrastructure, improve data security, and build staff capacity.

3. Conclusion

The findings indicate a pressing need for digital transformation within the justice sector to enhance service delivery and support the goals of the Chilungamo II Programme. The implementation of recommended actions will lead to more efficient case management, improved data security, and better access to justice, particularly for marginalized communities.

List of Acronyms

AWP	Annual Work Plan
CA	Contracting Authority
CJCC	Criminal Justice Coordinating Committee
CSO	Civil Society Organisations
CSU	Court Users Committee
CVSU	Community Victim Support Unit
DDP	Directorate of Public Prosecutions
DGS	Democratic Governance Sector
DGSS	Democratic Governance Sector Strategy
DP	Development Partner
EUD	European Union Delegation
GoM	Government of Malawi
KE	Key Expert
KRA	Key Result Area
LAB	Legal Aid Bureau
MHRC	Malawi Human Rights Commission
MoJ	Ministry of Justice
NAO	National Authorising Office / Officer
NICE	National Institute for Civic Education
NIP	National Indicative Programme
NKE	Non-Key Expert
NRB	National Registration Bureau
OWP	Overall Work Plan
PAO	Public Attorney's Office
PMU	Programme Management Unit
PPU	Project and Planning Unit
PSC	Programme Steering Committee
SG	Solicitor General
SWAp	Sector Wide Approach
SWG	Sector Working Group
STE	Short-Term Expert
TA	Technical Assistance
TL	Team Leader
ToA	Timetable of Activities
ToR	Terms of Reference
UNDP	United Nations Development Programme
UNICEF	United Nations Children's Fund
VSU	Victim Support Unit
WG	Working Group
WP	Work Plan

Contents

1. Introduction

1.1 Background

The Chilungamo II Programme, funded by the European Union, seeks to strengthen access to justice, promote human rights, and enhance accountability in Malawi. The success of this program is contingent upon the ability of justice institutions to adopt digital systems that improve operational efficiency and service delivery. This report consolidates the findings from a comprehensive ICT needs assessment conducted across key justice institutions in Malawi.

1.2 Scope of Work

This report focuses on the ICT infrastructure, network capabilities, data security protocols, and staff ICT skills within the Ministry of Justice, Malawi Legal Aid Bureau, Malawi Police Service, Malawi Human Rights Commission, Office of the Ombudsman, and Malawi Prisons Service. The scope includes detailed analysis of the institutions' current ICT state, challenges, and recommendations for future improvement.

2. Objectives

2.1 Mission Objectives

The objectives of the ICT assessment were to:

- Evaluate the current state of ICT infrastructure across the five institutions.
- Identify gaps in data security, network connectivity, and ICT skills among staff.
- Provide actionable recommendations for improving digital capacity and service delivery.
- Enhance case management and data security systems.

2.2 Expected Results

The assessment aimed to deliver a set of actionable recommendations that will improve operational efficiency through digital transformation, enhance data security, and enable justice institutions to better serve the public.

3. Methodology

3.1 Approach

The assessment employed a combination of surveys, interviews, and field observations to collect data on the ICT infrastructure and operations within the institutions. The methodology also involved document reviews and stakeholder consultations to gain deeper insights into operational challenges.

3.2 Data Collection

Data was collected using:

- **Surveys**: Administered to ICT staff to evaluate current equipment, software usage, and network infrastructure.
- **Interviews**: Conducted with institutional leaders, IT managers, and staff to gather qualitative insights on the challenges faced.

- **Field Visits**: Visits to regional offices to assess the physical state of ICT infrastructure and observe operational practices.

3.3 Analysis

The data was analyzed to identify key gaps in ICT infrastructure, data security, and staff capacity. Recommendations were developed based on best practices and aligned with the goals of the Chilungamo II Programme.

4. Findings

4.1 Overview of Key Findings

- The assessment found significant deficiencies in ICT infrastructure across all institutions. Most of the hardware is outdated, network connectivity is unreliable, and data security protocols are weak or non-existent.

4.2 Detailed Findings

4.2.1 ICT Infrastructure

Across all assessed institutions, a significant portion of ICT hardware is outdated, with some equipment being over five to ten years old. This leads to frequent breakdowns, slow processing times, and inability to run modern software applications necessary for efficient case management and data processing.

- **Malawi Legal Aid Bureau**: Outdated desktops and laptops, particularly in regional offices.
- **Malawi Police Service**: Over 50% of hardware is outdated, affecting productivity.
- **MHRC**: Desktops and laptops are over five years old, hindering case processing.
- **Office of the Ombudsman**: Hardware is between 4 to 10 years old, reducing efficiency.
- **Malawi Prisons Service**: Only 25% of computers are fully functional.
- **Ministry of Justice:** Outdated hardware; poor network reliability.

4.2.2 Data Security and Privacy

Data security protocols are either weak or non-existent, exposing sensitive data to risks of breaches or loss. Many institutions lack formal disaster recovery plans and rely on manual backups, which are insufficient for safeguarding critical information.

- **Lack of Encryption**: Sensitive data is often stored without encryption, making it vulnerable.
- **Manual Backups**: Increase the risk of data loss due to human error or hardware failure.
- **Use of Unlicensed Software**: Poses legal risks and security vulnerabilities.

4.2.3. ICT Skills and Training

Staff in most institutions lack advanced ICT skills, particularly in cybersecurity, data management, and specialized software applications. There is limited or no structured training in place to enhance these skills, leading to over-reliance on external vendors and delayed problem resolution.

4.2.4. ICT Support

ICT support teams are generally understaffed and lack the capacity to manage the institutions' technical needs effectively. The absence of structured helpdesk systems results in uncoordinated issue reporting and prolonged downtimes.

5. Challenges

5.1 Identified Challenges

- **Outdated Hardware**: Many institutions rely on aging computers and network devices, which severely limits operational efficiency.
- **Network Connectivity**: Frequent network downtime affects communication and case management.
- **ICT Staff Capacity**: Insufficient ICT training for staff exacerbates technical issues and delays problem resolution.
- **Data Security Risks**: Expose sensitive information to potential breaches, undermining public trust and potentially violating privacy laws.
- **Manual Processes**: Lead to delays, inaccuracies, and increased operational costs.

5.2 Mitigation Measures

- Immediate replacement of outdated hardware and network upgrades.
- Introduction of data security protocols, including encryption and automated backups.
- Training programs for staff to improve ICT competencies.

6. Impact of ICT Deficiencies on Access to Justice

6.1 Delayed Justice Delivery

The lack of digital case management systems results in prolonged case handling times. Manual record-keeping leads to misplacements, loss of files, and difficulty in tracking case progress, violating the legal maxim that "justice delayed is justice denied."

6.2 Inequitable Access

Citizens in rural and remote areas face significant barriers in accessing justice services due to geographical distances and the absence of online platforms that could bridge this gap. The digital divide exacerbates inequalities, leaving marginalized groups without adequate legal support.

6.3 Reduced Efficiency and Increased Costs

Inefficient processes strain institutional resources, leading to increased operational costs. These costs are often passed on to the citizens indirectly, making access to justice more expensive and less attainable for the economically disadvantaged.

6.4 Erosion of Public Trust

Frequent data breaches or loss of sensitive information due to weak security measures undermine public confidence in justice institutions. This distrust discourages citizens from seeking legal recourse, perpetuating a cycle of injustice.

6.5 Hindrance to Economic Development

A robust justice system is essential for economic growth, providing a stable environment for business and investment. ICT deficiencies impede the enforcement of contracts, protection of property rights, and resolution of disputes, deterring economic activities.

7. Recommendations

7.1 Immediate Actions (0-12 Months)

7.1.1 Hardware Upgrades

- Replace outdated computers, laptops, and printers in critical departments.
- Prioritize regional offices to enhance service delivery (access to justice) in rural areas.

7.1.2 Network Improvements

- Upgrade network infrastructure by installing modern routers and switches.
- Ensure reliable internet connectivity across all offices.
- Expand LAN and Wi-Fi coverage to eliminate connectivity blind spots.

7.1.3 Cybersecurity Measures

- Implement basic cybersecurity protocols, including firewalls and antivirus software.
- Begin encryption of sensitive data to protect against unauthorized access.
- Develop and enforce strong password policies.

7.1.4 Staff Training

- Conduct immediate training workshops on basic ICT skills and cybersecurity awareness.
- Focus on training staff in the use of essential software applications.

7.2 Medium-Term Actions (12-36 Months)

7.2.1 Implement Case Management Systems

- Develop or acquire centralized digital case management systems tailored to each institution's needs.

- Ensure systems are user-friendly and accessible to staff with varying ICT competencies.

7.2.2 Continuous ICT Training Programs

- Establish structured training programs to continually enhance staff ICT skills.
- Include specialized training in data management, cybersecurity, and use of advanced software.

7.2.3 Expand ICT Support Teams

- Recruit additional ICT personnel to improve technical support and reduce downtime.
- Implement helpdesk systems for efficient issue tracking and resolution.

7.2.4 Data Security Enhancements

- Develop comprehensive data security policies.
- Implement automated backup systems with offsite storage options.
- Regularly update and patch software to protect against vulnerabilities.

7.3 Long-Term Goals (36-60 Months)

7.3.1 Develop Disaster Recovery Plans

- Create and regularly test disaster recovery and business continuity plans.
- Ensure critical systems can be restored promptly in the event of a failure.

7.3.2 Establish ICT Policies and Governance

- Develop overarching ICT policies covering hardware lifecycle management, software licensing, network usage, and data governance.
- Align policies with national ICT strategies and legal requirements.

7.3.3 Promote Digital Inclusion

- Develop online platforms and mobile applications to increase accessibility of justice services.
- Provide public education on accessing digital services, particularly targeting rural and marginalized communities.

7.3.4 Monitor and Evaluate ICT Initiatives

- Implement monitoring and evaluation frameworks to assess the effectiveness of ICT interventions.
- Use feedback to continuously improve systems and processes.

8. Conclusion

8.1 Achievement of Objectives

The assessment successfully identified the key ICT deficiencies across the justice institutions and provided actionable recommendations for addressing them. The implementation of these recommendations will significantly improve the efficiency of justice delivery and enhance data security.

8.2 Next Steps

The next steps include prioritizing the immediate actions, particularly hardware replacements and network upgrades, followed by the implementation of case management systems and continuous ICT training programs.

9. Annexes

Annex A: Detailed ICT Equipment Inventories

This annex provides a detailed inventory of ICT equipment across the various justice institutions assessed. It highlights the current state of hardware and software infrastructure, identifies functionality issues, and outlines the actions required for each institution.

A.1 Malawi Legal Aid Bureau ICT Inventory

Equipment Type	Condition	Quantity	Location	Remarks/Action Required
Desktops	Good	120	Lilongwe HQ	No immediate action required
Laptops	Fair	80	Blantyre	Replace within the next 12 months
Printers	Poor	10	Regional	Immediate replacement needed
Routers	Fair	15	All Offices	Replace outdated routers
Network Switches	Poor	5	Lilongwe HQ	Upgrade to enhance network performance

A.2 Malawi Police Service ICT Inventory

Equipment Type	Condition	Quantity	Location	Remarks/Action Required
Desktops	Fair	500	Various Police Offices	Replacement required for 50% of devices
Laptops	Fair	50	Manager Offices	Immediate repairs and upgrades needed
Servers	Good	10	Data Center	Adequate, but underutilized
Printers	Needs Repair	30	Admin Offices	Frequent issues, servicing required
Routers/Switches	Outdated	25	Various Departments	Upgrade required for faster performance

A.3 Malawi Human Rights Commission (MHRC) ICT Inventory

Equipment Type	Condition	Quantity	Location	Remarks/Action Required
Desktops	Fair	10	Main Office (Lilongwe)	Replace outdated units
Laptops	Fair	56	Various Departments	Immediate repairs for malfunctioning units
Printers	Outdated	23	Various Departments	Replace outdated units for efficiency
Network Devices	Poor	15	MHRC Offices	Upgrade network devices for stability
Scanners	Good/Fair	3	Legal and Accounts Depts	Regular servicing required

A.4 Office of the Ombudsman ICT Inventory

Equipment Type	Condition	Quantity	Location	Remarks/Action Required
Desktops	Outdated	40	Lilongwe HQ and Regional Offices	Immediate replacement required
Laptops	Functional	15	Regional Offices	Upgrade needed for half of devices
Printers	Needs Repair	8	Lilongwe HQ	Frequent breakdowns, requires servicing
Servers	Non-functional	2	Central Server Room	Replacement and repair needed

A.5 Malawi Prisons Service ICT Inventory

Equipment Type	Condition	Quantity	Location	Remarks/Action Required
Desktops	25% Functional	40	Prisons HQ	Immediate replacement for 75% of units
Laptops	50% Functional	15	Admin Departments	Urgent repairs or replacements required
Servers	Non-functional	2	Data Center	Replacement required for full functionality

Routers/Switches	Functional	10	Various Locations	Some areas require coverage extension
Network Access Points	60% Functional	10	Prisons HQ and Regional Offices	Upgrade for better network coverage

Annex B: Network Infrastructure Assessments

This annex assesses the network infrastructure within the institutions, outlining the current state of network coverage, bandwidth capacity, and areas where network improvements are required.

B.1 Malawi Legal Aid Bureau Network Infrastructure

Network Component	Current State	Recommendation
Internet Bandwidth	Low, frequent disruptions	Increase bandwidth, especially in regional offices
LAN Coverage	Partial in regional offices	Extend LAN coverage to ensure stable connectivity
Wi-Fi Coverage	Inconsistent	Install additional access points to improve Wi-Fi reach
Network Devices (Routers)	Outdated	Replace outdated routers and switches to improve performance

B.2 Malawi Police Service Network Infrastructure

Network Component	Current State	Recommendation
Internet Bandwidth	Limited	Upgrade to higher bandwidth to meet operational demands
Network Downtime	Frequent	Address connectivity issues through infrastructure improvements
Wireless Network (Wi-Fi)	Poor in high-traffic areas	Expand Wi-Fi coverage to improve access in all departments
Security Firewalls	Weak	Implement robust firewalls to secure sensitive data

B.3 Malawi Human Rights Commission (MHRC) Network Infrastructure

Network Component	Current State	Recommendation
Internet Bandwidth	Moderate	Improve stability with higher capacity broadband
Wireless Network	Limited Coverage	Extend Wi-Fi coverage to all departments

Routers/Switches	Outdated	Replace outdated network devices for stable performance

B.4 Office of the Ombudsman Network Infrastructure

Network Component	Current State	Recommendation
Internet Bandwidth	Frequent Downtime	Increase bandwidth and improve connectivity
LAN Coverage	Inconsistent	Extend LAN coverage to improve access in regional offices
Wi-Fi Coverage	Limited	Install additional access points for full coverage
Security Measures	Weak	Upgrade firewalls and implement network monitoring tools

B.5 Malawi Prisons Service Network Infrastructure

Network Component	Current State	Recommendation
Internet Bandwidth	Less than 10 Mbps	Upgrade to a more stable broadband connection
LAN Coverage	Limited to administrative areas	Expand LAN and Wi-Fi coverage to operational areas
Routers/Switches	70% Functional	Upgrade routers and switches for better performance
Firewalls	Basic	Install advanced firewalls to protect against data breaches

Annex C: Data Security Audit Reports

This annex details the findings of data security audits conducted within the institutions. It highlights vulnerabilities, current practices, and recommendations for improving data security and privacy.

C.1 Malawi Legal Aid Bureau Data Security Audit

Security Measure	Current State	Risk Level	Recommendation
Data Backups	Manual	High	Implement automated backup systems
Encryption	None	High	Encrypt sensitive data

Firewall Protection	Basic	Medium	Install advanced firewalls
Software Licenses	Unlicensed (Cracked)	High	Transition to licensed software

C.2 Malawi Police Service Data Security Audit

Security Measure	Current State	Risk Level	Recommendation
Data Backups	Inconsistent	High	Implement regular automated backups
Cybersecurity Training	Minimal	High	Conduct staff training on data security
Firewalls	Weak	Medium	Install robust firewalls to prevent breaches
Incident Response Plan	None	High	Develop a formal incident response plan

C.3 Malawi Human Rights Commission (MHRC) Data Security Audit

Security Measure	Current State	Risk Level	Recommendation
Backup Systems	Manual	High	Automated backups required
Encryption	Not in place	High	Encrypt all sensitive case files
Antivirus Software	Outdated	Medium	Regularly update antivirus and patch systems
Cybersecurity Awareness	Low	High	Immediate training on cybersecurity risks

C.4 Office of the Ombudsman Data Security Audit

Security Measure	Current State	Risk Level	Recommendation
Data Backups	Manual	High	Introduce automated cloud backup systems
Encryption	None	High	Secure data with encryption protocols
Disaster Recovery Plan	None	High	Develop and test a disaster recovery plan
Cybersecurity Protocols	Weak	Medium	Strengthen cybersecurity protocols

C.5 Malawi Prisons Service Data Security Audit

Security Measure	Current State	Risk Level	Recommendation
Backup Systems	None	High	Implement regular automated backups
Firewalls	Basic	Medium	Install advanced firewalls and VPN
Cybersecurity Training	Low	High	Immediate cybersecurity training for staff
Incident Response Plan	None	High	Develop a formal incident response plan

Annex D: Training Needs Assessments

This annex outlines the ICT skills assessment across institutions and provides recommendations for training and capacity building.

D.1 Malawi Legal Aid Bureau ICT Training Needs

Skill Area	Current Proficiency Level	Training Required
Basic ICT Skills	High	Regular refresher courses
Cybersecurity Awareness	Low	Immediate cybersecurity awareness training
Data Management	Low	Training in database management
Network Administration	Low	Focused training on network maintenance

D.2 Malawi Police Service ICT Training Needs

Skill Area	Current Proficiency Level	Training Required
Cybersecurity	Low	Regular training on data protection
Case Management Software	Low	Training in digital case management
Data Management	Low	Improve skills in data entry and management
Advanced ICT Skills	Low	Immediate training on advanced ICT solutions

D.3 Malawi Human Rights Commission ICT Training Needs

Skill Area	Current Proficiency Level	Training Required
Cybersecurity	Medium	Continuous training on advanced threats

Data Privacy	Low	Training on GDPR and data privacy laws
Network Maintenance	Low	Training on network security and maintenance
Case Management Software	Low	Training on digital case management systems

D.4 Office of the Ombudsman ICT Training Needs

Skill Area	Current Proficiency Level	Training Required
Cybersecurity	Low	Immediate focus on data security training
ICT System Management	Low	Training on managing case management systems
Data Security Awareness	Low	Training on encryption and secure data handling

D.5 Malawi Prisons Service ICT Training Needs

Skill Area	Current Proficiency Level	Training Required
Basic ICT Skills	Moderate	Regular refresher courses
Data Management	Low	Training on database management for inmate records
Network Administration	Low	Training on improving network connectivity

Annex E: Case Studies

E.1 Malawi Police Service: Impact of ICT Deficiencies on Case Management

This case study highlights how the lack of a centralized case management system in the Malawi Police Service results in delayed case processing and challenges in tracking and managing cases, especially across different regions. By adopting digital systems, the police force can streamline operations and significantly reduce case backlogs.

E.2 Malawi Prisons Service: Inefficiencies in Inmate Record Management

The absence of specialized inmate management software has led to inefficiencies in maintaining accurate records, with frequent errors in manual record-keeping. This case study explores how the adoption of a centralized inmate management system can improve service delivery, reduce errors, and enhance overall prison administration.

Annex F: Stakeholder Engagement

This annex lists the stakeholders consulted during the ICT assessment and provides a summary of their insights.

F.1 List of Stakeholders

- **Malawi Legal Aid Bureau**: Director of ICT, Head of Operations, Senior Legal Aid Officers
- **Malawi Police Service**: Chief of ICT, Senior Police Officers, Network Administrators
- **Malawi Human Rights Commission**: ICT Manager, Human Rights Officers, Administrators
- **Office of the Ombudsman**: Director of ICT, Ombudsman Staff, Legal Advisors
- **Malawi Prisons Service**: Head of ICT, Inmate Records Officers, Regional Prison Administrators

F.2 Key Insights

- **General Consensus**: All institutions face significant challenges in digitalizing their services due to outdated infrastructure and limited staff training.
- **Recommendations**: Stakeholders emphasized the need for immediate investment in ICT infrastructure, staff capacity building, and system integration.