THE UNITED REPUBLIC OF TANZANIA
NATIONAL AUDIT OFFICE

ANNUAL GENERAL REPORT OF THE CONTROLLER AND AUDITOR GENERAL

ON THE AUDIT OF THE INFORMATION SYSTEMS FOR THE YEAR ENDED 30TH JUNE, 2018

UNITED REPUBLIC OF TANZANIA

NATIONAL AUDIT OFFICE

The Controller and Auditor General, National Audit Office, P.O. Box 950, 41104 Tambukareli Dodoma. Telegram: "Ukaguzi", Telephone: +255 (026) 2321759, Fax: +255(026)2117527, E-mail: ocag@nao.go.tz, Website: www.nao.go.tz

28 March, 2019

In reply please quote
Ref.No. GA.27/180/02

Dr. John Pombe Joseph Magufuli,
The President of the United Republic of Tanzania,
State House,
P.O. Box 9120,
1 Barack Obama Road,
11400 DAR ES SALAAM.

Your Excellency,

Re: Submission of General Report of the Controller and Auditor General on the audit of information systems for the year ended 30th June, 2018

Pursuant to Article 143(4) of the Constitution of the United Republic of Tanzania of 1977 (as amended from time to time) and Sec.34 (1) (c) of the Public Audit Act 2008, I hereby submit to you for the first time my standalone Annual General Report on audit of information systems for the year ended 30th June, 2018.

I submit.

Prof. Mussa J. Assad
CONTROLLER AND AUDITOR GENERAL

Mandate

The statutory duties and responsibilities of the Controller and Auditor General are provided for under Article 143 of the Constitution of the URT of 1977 (revised 2005) and in Sect. 10 (1) of the Public Audit Act, 2008.

Vision

To be a highly regarded Institution that excels in Public Sector Auditing.

Mission

To provide high quality audit services that improves public sector performance, accountability and transparency in the management of public resources.

Core Values

In providing quality services, NAO is guided by the following Core Values:

- ✓ **Objectivity:** We are an impartial public institution, offering audit services to our clients in unbiased manner.
- ✓ **Excellence:** We are professionals providing high quality audit services based on standards and best practices.
- ✓ **Integrity:** We observe and maintain high standards of ethical behaviour, rule of law and a strong sense of purpose.
- ✓ **People focus:** We value, respect and recognize interest of our stakeholders.
- ✓ **Innovation:** We are a learning and creative public institution that promotes value added ideas within and outside the institution.
- ✓ **Results Oriented:** We are an organization that focuses on achievement based on performance targets.
- ✓ **Team work Spirit:** We work together as a team, interact professionally, share knowledge, ideas and experiences.

We do this by: -

- Contributing to better stewardship of public funds by ensuring that our clients are accountable for the resources entrusted to them;
- Helping to improve the quality of public services by supporting innovation on the use of public resources;

- Providing technical advice to our clients on operational gaps in their operating systems;
- Systematically involve our clients in the audit process and audit cycles; and
- Providing audit staff with appropriate training, adequate working tools and facilities that promote their independence.

© This audit report is intended to be used by Government Authorities. However, upon receipt of the report by the Speaker and once tabled in Parliament, it becomes a public record and its distribution may not be limited.

TABLE OF CONTENTS

List of Abbreviations ..... **v**
Preface ..... **vii**
Acknowledgements ..... **ix**
EXECUTIVE SUMMARY **1**
CHAPTER ONE **8**
BACKGROUND AND GENERAL INFORMATION **8**
1.0 INTRODUCTION **8**
1.1 Audit Mandate and Rationale for Audit 9
1.2 Responsibilities of the Controller and Auditor General 9
1.3 Scope and Applicable Audit Standards 10
1.4 Organization of Audit Work 11
CHAPTER TWO **12**
2.0 EFFECTIVENESS OF THE INFORMATION SYSTEMS **12**
2.1 Inadequate segregation of duties 12
2.2 ICT systems Interface and Integration 15
2.3 Non Consideration of Underlying Policy and Regulations 18
2.4 Inadequate application access and change controls 21
CHAPTER THREE **25**
3 EFFICIENCY OF INFORMATION SYSTEMS **25**
3.1 Operations not performed within the Systems 25
3.2 Government visibility over transactions 29
3.3 Assessment of reliability of systems 30
CHAPTER FOUR **32**
4 MANAGEMENT OF ICT SYSTEMS AND PROJECTS **32**
4.1 Duplication of Efforts in implementing ICT Systems 32
4.2 Systems underutilization 33
4.3 Inadequate risk management 36
4.4 Inadequate ICT projects management 37
4.5 Inadequate ICT governance 40
4.6 Lack of internal information systems audit 42
4.7 Inadequate IT general controls 43
CHAPTER FIVE **48**
5.0 GENERAL CONCLUSION AND RECOMMENDATIONS **48**
5.1 General Conclusion **48**
5.2 General Recommendations **51**
ANNEXURES **52**
Annexure 1: Summary of Audit findings with their respective risk rating 52

Table of figures

Figure 1: IT Audit findings' reporting Framework 11

List of Abbreviations

AFROSAI-E	African Organization of Supreme Audit Institutions - English speaking Countries
AOs	Accounting Officers
BCP	Business Continuity Plan
BRELA	Business Registrations and Licensing Agency
CAATs	Computer Assisted Audit Techniques
CAG	Controller and Auditor General
DART	Dar es Salaam Bus Rapid Transit
DRP	Disaster Recovery Plan
EDAMS	Engineering Design Analysis Management System
GBT	Gaming Board of Tanzania
GePG	Government Electronic Payment Gateway
GSPP	Government Salary Payment Platform System
HCMIS	Human Capital Management Information System
ICT	Information and Communications Technology
IFMS	Integrated Financial Management Systems
IPSAS	International Public Sector Accounting Standards
IT	Information Technology
LAAC	Local Authority Accounts Committee (LAAC)
LGAs	Local Government Authorities
LGFM	Local Authority Financial Memorandum
LGFM	Local Government Financial Memorandum
LPO	Local Purchase Order
MC	Municipal Council
MDAs	Ministries, Departments and Agencies
MDG	Millennium Development Goals
MNH	Muhimbili National Hospital
MoFP	Ministry of Finance and Planning
MoU	Memorandum of Understanding
NAOT	National Audit Office of Tanzania
PAC	Public Accounts Committee
PAs	Public Authorities

PAs	Public Authorities
PFA	Public Finance Act (No. 6 of 2001 revised 2004)
PFR	Public Finance Regulations
PO-PSM	President's Office Public Service Management
PO-RALG	President's Office Regional Administrative Local Government
PSP	Payment Service Providers
SNAO	Swedish National Audit Office
SPs	Service Provider
SUMATRA	Surface and marine Transport Regulatory Authority
SURLIS	Surface Registration and License Information System
TASAF	Tanzania Social Action Fund
TBS	Tanzania Bureau of standards
TIB	Tanzania Investment Bank
TPB	Tanzania Postal Bank
TRA	Tanzania Revenue Authority
TSA	Treasury Single Account
UDART	Usafiri Dar es Salaam Rapid Transit
URT	United Republic of Tanzania

Preface

This Annual General Report for information systems is a summary of results on the audits of information systems for the year ended 30th June, 2018. This is the first annual general report of information systems which comprises of three major information systems and IT general controls surrounding these systems. The three information systems are LGA IFMS Epicor at PO-RALG, HCMIS Lawson at PO-PSM and GePG at MoFP. In addition the report includes audits of information systems with their IT general controls of Public Authorities and ICT project management.

The report was prepared and submitted to the President of the URT in accordance with Article 143 of the Constitution of the URT of 1977 (as amended from time to time) and Sect. 34(1) & (2) of the Public Audit Act, 2008. It contains a summary of main findings that were separately issued in detailed management letters and audit reports to the managements of MDAs and PAs.

It is my expectation that the report would assist the government of URT to assess challenges identified in implementation of information systems and adoption of ICT in the government of URT to ensure improvement of government operations and enhancement of internal controls to realize value for money.

Pursuant to Article 143(2)(c)& (4) of the Constitution of the URT of 1977 (as amended from time to time) the Controller and Auditor General is required to audit at least once a year and submit to the President of the URT every report he makes that are later tabled to the Parliament.

Operational independence of the NAOT has improved following the enactment of the Public Audit Act, 2008 and the Public Audit Regulations 2009. However, there is a need of improvement for working resources in order to effectively discharge my constitutional mandate and obligations.

I hope that the Government, Parliament, Development Partners and the Public in general will find this report useful in knowing how the information systems and adoption of ICT is managed by the Accounting Officers and other information systems users.

Prof. Mussa J. Assad
CONTROLLER AND AUDITOR GENERAL

National Audit Office of Tanzania,
Dodoma.
March, 2019

Acknowledgements

I appreciate the support given to my office by the key stakeholders that enabled us to carry out our constitutional obligation; they include the Parliamentary Oversight Committees such as Public Accounts Committee (PAC) and Local Authority Accounts Committee (LAAC) and the Paymaster General, Accounting Officers in respect of MDAs, Local Government Authorities (LGAs) and Public Authorities (PAs) who manage information systems.

My sincere appreciations go to all NAOT staff for their dedicated hardworking and due diligence to accomplish this constitutional commitment. It is my hope that they will continue to provide efficient and effective audit services in order to enhance transparency and accountability in the collection and use of public resources.

I would like to extend my special appreciation to the development partners particularly the World Bank (WB), PFMRP and all other well-wishers that contributed their funds for capacity building and working resources towards modernization of audit functions.

Lastly, I would like to thank the Printer for expeditiously publishing this report.

EXECUTIVE SUMMARY

Government has increasingly computerized its processes to promote more efficient and effective government operations, facilitate more accessible government services, allow greater public access to information and make government more accountable to citizens. However, these computerized processes need to be audited to determine whether the intended objectives have been achieved.

I have audited Information Technology (IT) systems in the financial year ended 30th June 2018. The audit covered three major IT systems and general controls surrounding these systems namely LGA IFMS Epicor at PO-RALG, HCMIS Lawson at PO-PSM and GePG at MoFP. In addition the report includes audits of information systems with their IT general controls of Public Authorities, MDAs and ICT project management. The objective of IT audits include: Ascertaining the level of compliance with the applicable laws, policies and standards in relation to IT; evaluating the reliability of data from IT systems which have an impact on the financial statements of the organizations; and Checking if there are instances of inefficiencies in the use and management of IT systems.

This general report provides a summary of main findings derived from 17 individual audits conducted in information systems whose audit reports have been separately issued to the Accounting officers. Assessment of the risk as per audit findings shows that 21 cases rated high while 18 cases rated medium, there were no cases rated low. The following are the main findings from the audit conducted:

Assessment of the IT systems effectiveness reveals control weaknesses relating to segregation of duties. District/Municipal Council Treasurers have access rights in LGA's IFMS Epicor system to enter budget, allocate fund, create, approve and post vouchers. In addition, they also do process payments. Assigning of conflicting access rights to one person at once violates segregation of duties which may lead to misuse. The review payment process in LGA IFMS Epicor system revealed that, system provides disbursement numbers and automatically creates TISS file to be sent to BOT and affecting the customer bank accounts. I have noted that payments can be voided without proper authority while they have already been paid.

Control weaknesses have been noted in accounting and revenue collection systems of Public Authorities. Accounting system at Tanzania Bureau of Standards (TBS) has not been configured to prevent user from posting transaction which the same user has prepared. A user can create/prepare and approve/verify/post a transaction at the same time. Review of Electronic Payment System at TBS noted that 192 out of 44,280 invoices were generated, approved and verified by the same person.

Similarly, a walkthrough of the SURLIS system at SUMATRA noted that the three stages of issuing license can be done by one person in the system. One person can enter details of a vehicle, verify application details, approve and issue payment notification.

Equally, Tanzania Food and Drug Authority (TFDA) have a management information system (MIS) to manage, receive and approve applications for product registration. Review of certificates issued to registered products between 1st July 2017 and 30th June 2018 revealed that out of 2782 applications 41 applications were evaluated and audited by the same person, 15 applications were evaluated and approved by the same person and 230 applications were audited and approved by the same person.

My review of GePG generic billing portal noted that user with billing manager role can set deadline for payment of bill without approval which provide room for intentional mistakes. The process of generating bill in the system has no approval, after the bill manager creates the bill it directly gets control number from GePG engine.

Review of ICT systems also noted lack of interface and Integration. For example LGAs IFMS Epicor system does not have automatic interface with TISS thus leading to weaknesses which pose a risk of double payment. The review of payment process in LGAs IFMS Epicor system noted control weaknesses in resetting payments, cashier Accountant can reset payment which has been paid as a result regenerate disbursement number causing the same payment to be considered as a new payment. Similarly, LGAs IFMS Epicor and Treasury Single Account are not integrated, Review of the process of transferring LGAs funds from commercial banks to PO-RALG accounts at BOT noted inadequacy of controls in place to ensure that fund transfer done in IFMS Epicor

system reflects the actual physical funds transferred from commercial banks to BOT General Fund accounts through Treasury Single Account (TSA) system. HCMIS Lawson with Ajira portal and IFMS Epicor are not integrated. Ajira portal has been established to control recruitments process from early stages of application, interviews and recruitments. The system generates unique identification number for every recruited person which is used as an introduction of new employee to employers. Employers use it for hiring process in the HCMIS Lawson. There have been reported incidents of forged introduction letters from PSRS to employers which can lead to ghost workers in HCMIS Lawson due to lack of integration between recruitment portal and HCMIS Lawson.

Accounting software and revenue collection systems are not integrated. My audit of EWURA License and Order Information System (LOIS), DAWASCO Engineering Design Analysis Management System (EDAMS) and DART own source revenue collection system revealed that systems have not been integrated with accounting systems. Information of revenue collected is manually transferred to accounting system which is prone to human errors leading to inconsistences of information between accounting system and revenue collection system.

Non Consideration of Underlying Policy and Regulations resulting into existence of duplicate employees in HCMIS Lawson system. Also, the system allows net salary less than allowable amount. The interview with HCMIS Lawson application team noted that the application has been configured to prevent deductions less than one-third (1/3) of gross salary. However, review of list of employees with their net salary and gross salary from HCMIS noted 16,787 out of 526,498 employees with net salary less than one-third of the gross salary.

The audit reveals inadequate validation control over approval in HCMIS Lawson application. Ineffective functioning of Commitment Control in LGAs IFMS Epicor system whereby Budget balances in system had negative values; Expenditures were made outside approved budget and Cashbook had negatives balances in general ledger accounts.

It was also noted that access and change controls are insufficiently applied. Non-monitoring of privilege user accounts. User access rights not are periodically reviewed and absence of application role matrix which defines the mapping between business roles against application access rights to provide guideline during granting of access to users so as to avoid granting excessive access rights and ensuring segregation of roles is adhered to, during granting of access to users of the application.

Similarly, assessment of the information systems' efficiency reveals operations performed outside the Systems. Accounting officers have not been using implemented systems in approving important documents, requests and applications submitted to them. My review of accounting systems and application systems which facilitate management of core operations of MDAs, LGAs and PAs revealed that AOs approve on printed documents in manual files instead of approving both on paper and inside the system. Systems have not been designed to allow AOs to login and approve instead approvals in systems were entered by subordinate officer after approval of AO on paper. I encourage AOs to personally be approving inside systems and login to these systems to review what has been done to ensure what has been approved manually on paper is reflected in the system and maintain audit trails inside the systems. I further noted that LGAs IFMS Epicor system is incompliant with IPSAS requirement. LGAs IMFS Epicor accounting system is not used to record accurately Accounts Payables. The commitment control requires the availability of actual cash balances in the physical bank accounts before it allows transaction to go through contrary to IPSAS accrual requirement. Inconsistencies between accounting manuals and accounting systems have been noted in the Local Authority Accounting Manual (LAAM) against LGAs IFMS Epicor system.

My review revealed that exited transit goods are not validated in the TANCIS system. My audit review of TANCIS data for transit goods (Dry and Wet cargo) at Kabanga, Rusumo, Mutukula, Tunduma and Kasumulu borders noted 599 transactions (entries) which were not confirmed to exit the country in the TANCIS system. However, our review of transit documents and manual registers maintained at the respective borders, indicated that the goods physically exited the country, but were not validated in the TANCIS system due to control weaknesses

My assessment of the systems' reliability noted inconvenient billing systems for collecting government revenue. Review of Government Electronic Payment System (GePG) noted inconveniences of billing systems due to system unavailability, difficulties in generating bills especially for those online systems which customers have to generate bills themselves, failures of systems to provide control number, ineffective mechanism to receive and handle reported complaints and failure to generate controls number for bulk payments.

The assessment of overall ICT projects management reveals duplication of Efforts in ICT Systems under operation. For example, Government Salary Payment Platform (GSPP) system performs the same payroll validation as HCMIS system does. Equally, the Ministry of finance and planning (MoFP) have developed an online portal for employees to access and print their salary slips. The same functionality is available in the Watumishi portal developed by PO-PSM.

Systems underutilization has been also noted. For example, LGAs IFMS Epicor has asset and procurement modules that are not utilized. My review of the DAWASCO Engineering Design Analysis Management System (EDAMS) noted that the system has five modules but only three modules are used. Non-utilization of the two modules may result into corporation failing to identify water supplied to detect water loss and plan for line maintenance without water loss, as a result can lead to failure to reduce non-revenue water.

My review of revenue collection systems revealed lack of visibility of transactions for systems managed by service providers. In my audit of UDART bus fare collection system noted that DART's accountants have access to dashboard of the system which is used to collect electronic payment of bus fare. I am concerned that the dashboard can be configured in favor of service provider to only show what UDART wishes DART to see. There was no mechanism for DART to get assurance on the integrity of transactions displayed on the dashboard. Moreover, my interview with GEPG team I inquired about the mechanism in place to ensure mobile network providers adhered to deduction of 1.1% of transaction for each government payment done by general public using mobile network; I was informed that surprise checks are conducted once in a while. Surprise checks are not sufficient and effective,

mobile network operators should be monitored on real time to ensure they do not raise the percentage of deduction above the agreed rate in the contract. This poses a risk of undetected increase in percentage of deduction which will affect the general public.

Other issues that have been noted in the audit include inadequate ICT risk management; Lack of periodic ICT risk assessment and tracking of identified risks; risk register is not maintained and Vulnerability assessment not conducted in systems. Inadequate business continuity and disaster recovery plan to ensure timely and effective recovery of data in case of disaster. Also lack of skills of internal audit functions to conduct information systems audit.

Furthermore, my audit of four ICT projects noted noncompliance with ICT projects management best practices and guidelines issued by e-government Agency guidebook for managing ICT project and risks. Projects are vendor driven whereby vendors own projects operations instead of project team, lack of project documentations; Failure to transfer technology from vendors; Ineffective project planning and monitoring; Inadequate ICT governance where by ICT steering committee not formulated and Ineffective reporting structure of ICT function.

My general conclusion is that the government institutions have been embarking on adopting ICT to facilitate effective operations and service delivery. However, I am concerned on the following: management of ICT projects to acquire application systems to ensure they operate as expected to bring value, dependency on vendors for support and maintenance of acquired application systems, security and continuity of application systems, coordination among government entities to avoid duplication of application systems, integration of application systems to ensure consistency of information and efforts to ensure full utilization of acquired application systems. Control and compliance with existing policies and regulations have been inadequately safeguarded. Underutilization of the systems implies cost ineffectiveness of the investments made. Lack of coordinated efforts among MDA and PAs in implementing information systems which cut across entities increases cost to the government.

Based on my audit findings and conclusion, I recommend the following:

- Accounting officers to champion the use of ICT by ensuring they utilize implemented systems in their day to day operations
- Government institutions to strengthen controls in ensuring internal controls and information security controls are effectively considered during implementation of application systems
- MDAs and PAs to consider establishing information security office for managing security risks associated with adoption of ICT in their operations. This will also ensure smooth implementation of my recommendation above.
- E-government agency to effectively strengthen its operations to ensure there are no duplication of efforts in implementing information systems in the government.
- Government to establish ICT project coordination office under E-government agency to ensure large ICT projects are effectively managed and monitored.
- Strengthen internal audit functions by equipping them with skills to be able to audit information systems
- GePG team in collaboration with e-government agency to oversee billing systems to ensure their effectiveness in facilitating payment of revenue.
- Government to establish gaps of integrations especially for major application systems
- Business Continuity Plan and Disaster Recovery Plan to be given priority in government institutions to ensure continuity of operation during disaster

CHAPTER ONE

BACKGROUND AND GENERAL INFORMATION

1.0 INTRODUCTION

Many organizations have computerized their processes because they recognize the tremendous benefits that IT can bring to their operations and services. E-Government initiatives all over the world endeavor to integrate Information and Communication Technologies (ICT) to transform delivery of government services to their stakeholders by improving quality of services, accountability and efficiency. The Government of Tanzania has increasingly computerized its processes in order to promote more efficient and effective government, facilitate more accessible government services, allow greater public access to information and make government more accountable to citizens.

However, these computerized processes need to be audited to determine whether the intended objective has been achieved. An Information Technology (IT) audit is an audit of an organization's IT systems, management, operations and related processes.

An IT audit may be carried out in connection with a financial, compliance or performance audit. As the records, services and operations of many organizations are often highly computerized, there is a need to evaluate the IT controls in the course of normal audit of these organizations.

I have audited information systems in the financial year ended 30th June 2018. The audit covered three major information systems and IT general controls surrounding these systems. These three information systems are LGA IFMS Epicor at PO-RALG, HCMIS Lawson at PO-PSM and GePG at MoFP. In addition, the report includes conducted audits of information systems with their IT general controls of Public Authorities and ICT project management. The objectives of IT audits include:

- Ascertaining the level of compliance with the applicable laws, policies and standards in relation to IT;
- Evaluating the reliability of data from IT systems which have an impact on the financial statements of the organizations; and
- Checking if there are instances of inefficiencies in the use and management of IT systems.

This general report provides a summary of main findings derived from individual audits conducted in information systems whose audit reports have been separately issued to the Project Implementers.

1.1 Audit Mandate and Rationale for Audit

In discharging these duties, I am required by Section 10 of the Public Audit Act, 2008, to satisfy myself on whether collection of public monies safeguards public interest and that all expenditure of public monies has been properly authorized and applied to the purposes for which they were appropriated and that the laws, directions and instructions applicable thereto have been duly observed; and economy, efficiency and effectiveness have been achieved on the use of public resources.

1.2 Responsibilities of the Controller and Auditor General

My responsibility is to evaluate the IT systems to determine whether they are efficiently and effectively working and provide reliable information to users and properly managed to achieve their intended benefits.

I am required by Section 10 (2) of the Public Audit Act No. 11 of 2008 to satisfy myself that:

- Accounts have been prepared in accordance with the appropriate accounting standards and legal framework;
- Reasonable precautions have been taken to safeguard the collection of revenue, receipt, custody, disposal, issue and proper use of public property; and

- Law, directives and instructions applicable thereto have been duly observed and expenditures of public money have been properly authorized.

1.3 Scope and Applicable Audit Standards

1.3.1 Scope of Audit

The conducted audits covered the evaluation of the application controls, ICT governance, ICT project management, ICT risk management, IT general controls and other audit procedures considered necessary in arriving at an audit conclusion. The audits were carried out based on risk and materiality, therefore the audit findings are confined to the extent that records, documents and information that were made available to me for audit purposes.

1.3.2 Applicable Auditing Standards

NAOT is a member of the International Organization of Supreme Audit Institutions (INTOSAI) and the African Organization of Supreme Audit Institutions of English Speaking Countries (AFROSAI-E). Therefore, the applied audit procedures were in line with the International Standards of Supreme Audit Institutions (ISSAI) issued by INTOSAI and International Standards on Auditing (ISA) issued by the International Federation of Accountants (IFAC).

These standards require that I comply with ethical requirements of planning and performing of the audit to obtain reasonable assurance on whether the information systems controls are adequate and effective. Moreover, I applied procedures which are in line with ISO/IEC 27002 an international standard for Information technology security techniques and e-government agency guidelines.

1.4 Organization of Audit Work

In analyzing major issues noted in the IT audits conducted, I have summarized the audit findings in terms of systems' effectiveness, efficiencies, reliability and overall management of IT systems projects as compared with the intended goal as shown in *Figure 1*.

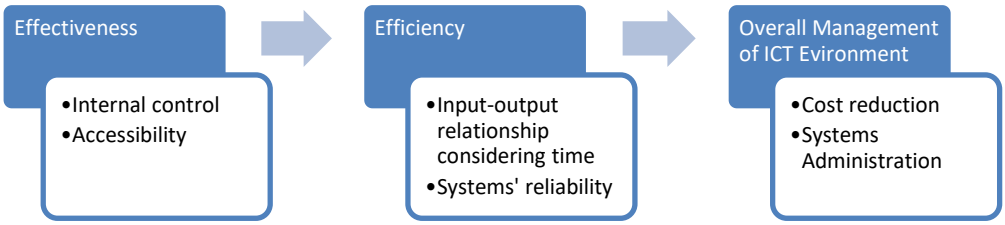

Figure 1: IT Audit findings' reporting Framework

This general report is structured into five chapters as follows: Chapter one provides background and general information; Chapter Two provides findings on the assessment of the effectiveness of the information systems; Chapter Three covers assessment of the information systems efficiency while Chapter Four covers assessment of the overall management of the IT systems projects. General conclusion and recommendations are presented in Chapter Five.

CHAPTER TWO

2.0 EFFECTIVENESS OF THE INFORMATION SYSTEMS

The review of the information systems to ascertain the level of compliance with the applicable laws, policies and standards revealed control and information security weaknesses as presented hereunder:

2.1 Inadequate segregation of duties

My review of application access controls of LGAs IFMS Epicor, accounting and revenue collection systems of Public Authorities noted the following control weaknesses associated with inadequate segregation of duties in these systems.

2.1.1 Control weakness noted in LGA's IFMS Epicor system

District/Municipal Council Treasurer have access right in LGA's IFMS Epicor system to enter budget, allocate fund, create, approve and post voucher. In addition, process payments. Assigning of conflicting access rights to one person at once violates segregation of duties which may lead to misuse.

Lack of approvals with respect to cancelation of payments in LGAs IFMS Epicor has also been noted. The review revealed that, system provides disbursement numbers and automatically creates TISS file to be sent to BOT and affecting the customer bank accounts. I have noted that payments can be voided without proper authority while they have already been paid.

In addition, the audit revealed control weaknesses over vendor creation process in LGAs IFMS Epicor system whereby same user can create and approve new vendor. IFMS Epicor is maintaining bank details of vendors to be used to pay vendors direct to their bank account through TISS, with this regard I am of the view that inadequate controls over creation and approval of vendor details can lead to

unauthorized payment or payment made to wrong vendor due to fictitious vendors.

2.1.2 Control weakness noted in accounting and revenue collection systems of Public Authorities

Accounting system at Tanzania Bureau of standards (TBS) has not been configured to prevent user from posting transaction which the same user has prepared. User can create/prepare and approve/verify/post transaction at the same time. Review of Electronic Payment System at TBS noted that 192 out of 44,280 invoices were generated, approved and verified by the same person. On inquiry I was informed by the management that this is caused by lack of enough employees thus one staff member has to generate, approve and verify invoices. However, in such case there should be a compensating control such as periodic review of user activities in the system to ensure they do not abuse the privilege.

Similarly, a walkthrough of the SURLIS system at SUMATRA noted that the three stages of issuing license can be done by one person in the system. One person can enter details of a vehicle, verify application details, approve and issue payment notification. I am concerned that intentional or unintentional human errors cannot be detected if both stages are done by one person.

Equally, Tanzania Food and Drug Authority (TFDA) have a management information system named MIS to manage receiving and approval of applications for product registration. The process of registering a product has six major steps; referencing whereby applicant details are filled, invoicing whereby invoice for payment of fee is prepared, accounting which involves account unit verifying payments, evaluation, auditing and final step is approval. Last three steps of Verification, auditing and approval of product registration are supposed to be done by three different persons in the system to ensure

segregation of duties. Review of certificates issued to registered products between 1st July 2017 and 30th June 2018 revealed that out of 2782 applications 41 applications were evaluated and audited by the same person, 15 applications were evaluated and approved by the same person and 230 applications were audited and approved by the same person.

These control weaknesses are attributed the lack of defined system role matrix and for those systems which have role matrix have not been incorporated in the design of the system.

I recommend management of PO-RALG, TBS, SUMATRA, TBS and TFDA to ensure all systems have defined role matrix as per responsibilities of users and make sure segregation of duties is considered in granting access rights to users of systems. For the cases where it is necessary for one person to be granted two conflicting roles at once due to shortage of staff then there should be periodic review of user activities in the system to detect abnormalities or abuse.

2.1.3 Control weaknesses noted in GePG generic billing portal

GePG has developed a generic billing portal to be used by SPs which do not have billing system to be able to generate bills and get control number for customers. The portal has basic functionalities for managing basic operations of bill creation since process of bill creation differs among SPs.

My review of the portal noted the following control weaknesses

- User with billing manager role can set deadline for payment of bill without approval. This provides room for intentional mistakes for personal gain. But, also can lead to inconsistency of deadlines among generated bills. Deadlines are required to be set by SP administrator during configuration of revenue sources to ensure consistency and authorization.
- The process of generating bill in the system lacks approval as a control tool. After the bill manager creates the bill, it directly gets control number from GePG engine. This can lead to fraud by assessing lower bill amount than actual amount. Any

assessment needs to be approved by responsible person to ensure segregation of duties to reduce human errors and intentional modification.

I recommend management of MoFP to (a) Implement configuration of bill deadline during configuration of revenue sources (b) implement approval of bills in the generic billing portal.

2.2 ICT systems Interface and Integration

My review evaluated how ICT systems under operations interface and integrate to maximize performance, efficiency and cost effectiveness. The audit revealed the following:

2.2.1 Weaknesses of interface between LGAs IFMS Epicor and TISS

The review of payment process in LGAs IFMS Epicor system noted control weaknesses in resetting payments. Cashier accountants have access to process payments which lead to creation of TISS file. The file is then uploaded by TISS up-loaders to BOT online TISS application for payment to be sent to recipient. Our review noted that Cashier Accountant can reset payment which has been paid before it has been posted. This regenerate disbursement number as a result the same payment is considered as a new payment which leads to double payment.

I recommend PO-RALG management to rectify IFMS Epicor to ensure it does not generate new disbursement number when payment is reset by accountant cashier.

2.2.2 LGAs IFMS Epicor and Treasury Single Account not integrated

PO-RALG manages nine bank accounts at the BOT which are shared by Local Government Authorities (LGAs). LGAs use these accounts for making payments but before payments are made they first transfer funds to these accounts from their own source revenue collection accounts at the commercial banks. Payments are done through

payment file generated by IFMS Epicor system after payment approvals, the payment file is then uploaded to BoT on Tanzania Interbank Settlement System (TISS).

Review of the process of transferring LGAs funds from commercial banks to PO-RALG accounts at BOT noted inadequacy of controls in place to ensure that fund transfer done in IFMS Epicor system reflects the actual physical funds transferred from commercial banks to BOT General Fund accounts through Treasury Single Account (TSA) system.

While users are required to quote the reference number of TISS transaction that transferred the funds during posting of the transfer (receipt) in IFMS Epicor, there are no checks to ensure that the TISS Reference number and transaction amount posted in IFMS Epicor are correct. Thus LGAs can post in IFMS Epicor more than what has been transferred as a result allows them to pay more than what they should since they are paying through consolidated accounts.

I am of the view that this is caused by lack of automated interface between LGAs IFMS Epicor and Treasury Single Account system to ensure the amount posted in IFMS Epicor is the same as the actual amount transferred to BOT. Absence of an automated control to check for correctness of the fund transfer increases the risk of overdraft since cashbook will allow LGAs to make payments while funds have not been received in PO-RALG BOT accounts.

I recommend management of PO-RALG and MoFP to coordinate efforts to establish automated interface between LGAs IFMS Epicor and TSA.

2.2.3 HCMIS Lawson with Ajira portal and IFMS Epicor not integrated

Ajira portal is the system developed under public services recruitment secretariat (PSRS). The system has been established to control recruitments process from early stages of application, interviews and recruitments. The system generates unique identification number for every recruited person which is used as an introduction of new

employee to employers. Employers use it for hiring process in the HCMIS Lawson. There have been reported incidents of forged introduction letters from PSRS to employers which can lead to ghost workers in HCMIS Lawson due to lack integration between recruitment portal and HCMIS Lawson.

Financial management information system (IFMIS Epicor) is the Government accounting system that controls Financials and budget controls including the government employee's salary bill. All human resources related cost should be reported in the IFMS Epicor. However HCMIS Lawson system has not been integrated with IFMS Epicor as a result the payroll payment controls follows manual intervention process which we believe it is costly, time consuming and subjected to human errors.

I am of the view that this is caused by lack of coordinated efforts among stakeholders. There is a risk that employers may employ wrong or fictitious employees due to lack of integration between HCMIS and recruitment portal. Moreover lack of integration with IFMS Epicor poses a possibility of spending beyond payroll approved budget.

I recommend management of PO-PSM to make sure that (a) HCMIS Lawson is integrated with other payroll supporting system; Ajira portal and IFMS Epicor (b) PO-PSM as a major stakeholder and regulator of ICT sector in government organizations to ensure coordinated efforts in implementing information systems

2.2.4 Accounting software and revenue collection systems not integrated

My audit of EWURA License and Order Information System (LOIS), DAWASCO Engineering Design Analysis Management System (EDAMS) and DART own source revenue collection system revealed that systems have not been integrated with accounting systems. Information of revenue collected is manually transferred to accounting system which is prone to human errors leading to inconsistences of information between accounting system and revenue collection system.

This is caused by non-consideration of full scope of implementation of revenue collection systems. Lack of integration between accounting system and revenue collection systems can compromise integrity of financial data and consequently lead to misstatements in the Financial Statements

I recommend management of EWURA, DAWASCO and DART to implement automatic interface between accounting system and revenue collection/billing system.

2.3 Non Consideration of Underlying Policy and Regulations

The system under operation is expected to be in line with the existing policy and regulations. However, the following non-compliance issues have been revealed.

2.3.1 Existence of duplicate employees in HCMIS Lawson system

My review of HCMIS Lawson system configurations of input validation controls specifically on preventing duplicate employees found that the system validates duplicate employees by using three employee names and birth date. However, this is ineffective as it is vulnerable to a small change since a change in single character of names or birthdate the system will consider that information as is of different employee thus it will not prevent such employee from entering in the system.

Further review of HCMIS Lawson revealed existence of 31 cases of duplicate employees who have the same first name, middle name, last name and birthdate but different check number. This is caused by lack of unique identification number such as national ID in the system to identify each employee uniquely. This may lead to ghost workers and double payment of salary.

2.3.2 HCMIS Lawson allows net salary less than allowable amount

According to circular number 3 paragraph 8.5 to public servants of 2011 regarding arrangement to lend loans to public servants requires

accounting officers during approving of staff loans to ensure staff should remain with one-third (1/3) of the gross salary after all deductions.

My interview with HCMIS Lawson application team noted that the application has been configured to prevent deductions less than one-third (1/3) of gross salary. However, review of list of employees with their net salary and gross salary from HCMIS noted 16,787 out of 526,498 employees have net salary less than one-third of the gross salary (Annexure 2 – Net pay less than one-third).

2.3.3 Inadequate validation control over approval of actions in HCMIS Lawson

My review of application controls over actions performed in the Lawson application such as promotions and registration of new employees noted that such actions are submitted by employers then reviewed and approved by PO-PSM staff in the system. However, forms which are used by employers to submit actions in the system have inadequate validation controls thus validations are left to approvers, such control deficiency in the process of submitting actions are:

(i) Scheme of services of entities cannot be captured in the system- which could have helped to prevent noncompliance with scheme of service during staff promotions and hiring. As a result of this there is dependency on approvers to ensure promotions submitted by employers are in accordance to scheme of service which is subjected to human errors.

(ii) "Ikama" is issued outside the system thus employers can employ or promote more staff than what has been approved which could have been prevented if "Ikama" was issued inside the system.

(iii) System allows users to select promotion from the action field while choosing position lower than the current employee's position.

However, dependency on approvers to detect wrong actions done by employers is subjected to human errors.

2.3.4 Nonfunctioning of Commitment Control in LGAs IFMS Epicor system

The audit of application controls of the IFMS Epicor system noted that the system has commitment controls which prevent users to perform unusual transactions. The system users shall not be able to process expenditures transaction and funds allocation until there is budget available in the system, funds availability in the selected line items Accounts and availability of cash book balances in the system. Review of itemized reports of LGAs as controlling tools of budget, funds, expenditure and cash management noted the following weaknesses:

a) Budget balances in system had negative values
b) Expenditures were made outsides approved budget and,
c) Cashbook had negatives balances in general ledger accounts

On inquiry, I was informed by the management that these weaknesses were caused by misbehavior of fund allocation and commitment processes/workflows in the Business Process Management (BPM) module of the IFMS Epicor system which requires restarting the process. Once the system experiences the above shortcomings, commitment controls placed in the system stop working until the system administrator intervenes by restarting the processes/workflows.

As a result, user of the system sometimes continues processing transaction in the system without commitments controls. In my view this may have an effect over the integrity of controls in place since payment passes even if there is no either budget or fund allocated. It compromises the concept of budget managements and Expenditure management.

2.4 Inadequate application access and change controls

2.4.1 Privilege user accounts not monitored

Section 10.10.2 of the ISO/IEC 27002 code of practice for information security management requires procedures for monitoring use of information processing facilities to be established and the results of the monitoring activities reviewed regularly.

My review of list of users with access to MHN hospital management information system noted that system administrators have full access to all modules for support purpose, with this regard regular review of system administrators' activities in the system is important to ensure there is no misuse. On inquiry about regular review and monitoring of system administrators' activities we were informed that review of system logs is done on daily basis but there was no report or evidence to substantiate that reviews are done.

I also reviewed systems changes done by administrator of Management Information System at TFDA, I noted that system does not log implemented changes done by system administrator as a result it was difficult to get assurance that requested changes were implemented as required, also system administrator's activities cannot be monitored. Furthermore, it was noted activities which are logged are database level activities however; periodic review of these activities was not done to detect violations during the year under review.

Similarly, the review of TIB Corporate revealed that there was no process in place to review audit trails, logs related to key system events. Activity logs for the privileged accounts on applications, operating system and database were not reviewed by an independent authority.

Absence of independent reviews of activity logs/audit trails of privileged accounts may lead to unauthorized activities and changes made to systems, parameters and data may go undetected. Hence, pose a major security threat and impact the confidentiality, integrity and availability of sensitive data.

I recommend management of MNH, TFDA and TIB corporate to ensure that system logs used to track administrator activity on systems is formally reviewed on a periodic basis by a competent official for any unapproved/prohibited activities. The reports should be signed off by the responsible official as evidence of review

2.4.2 Non review of user access rights

Section 11.2.4 of the ISO/IEC 27002 code of practice for information security management requires management to review users' access rights at regular intervals using a formal process.

My review of user access list of MNH Hospital Management Information System (Jeeva) noted more than 1500 users with different access levels to different modules of the system. Therefore regular review of access granted to users was crucial to ensure proper access rights have been granted to users as per their responsibilities and in accordance to internal policies. However, during the review it was revealed that review of user access rights has not been done.

The audit of TPB PLC ICT policy found that the policy requires the line managers to confirm correctness of user access rights to systems within their units on quarterly basis and inform the IT help desk manager. In my review I observed that although user access rights reviews were performed, there was no evidence to confirm that the line managers have communicated to the IT help desk results of their review. Without proper feedback channel in the user access rights review process, there is a risk that feedback from the line managers is not acted upon in a timely manner. I also noted the case of lack of regualar reviews of user access rights in my audit of TIB Corporate.

I recommend management of MNH, TPB PLC and TIB corporate to ensure user access rights are reviewed periodically by the departmental heads to ensure that employee system level access is commensurate with their job responsibilities and to maintain compliance with Information Policies.

2.4.3 Lack of documented application role matrix

Role matrix defines the mapping between business roles against application access rights to provide guideline during granting of access to users so as to avoid granting excessive access rights and ensuring

segregation of roles is adhered during granting of access to users of the application.

My audit of access controls to MNH Hospital Management Information System (Jeeva) and TBS accounting software revealed that there was no role matrix to ensure users of systems are granted access rights based on their responsibilities to avoid granting of excess privileges. Moreover, my review of the same at TIB development bank noted the bank has not established segregation of duties document that guides the process of granting access to users in SmartStream system in accordance with the business rules.

I recommend management of MNH, TBS and TIB Development bank to establish role matrix document for all applications in the organization.

2.4.4 Inadequate application change controls

TIB Development bank limited ICT security policy on system change management states that every change should be defined in either of the three categories; Type A, type B and type C. The approval procedures of the change will depend on the type of the change. Furthermore it states that after live implementation of the change business owners are supposed to review if the change satisfies their business requirements.

I inspected two out of three change request forms and noted that both change request forms did not include a field that specifies the type of change so as to govern the approval required. Moreover I noted that for the both change request forms inspected there was no a sign-off from business owners after live implementation to confirm whether the change satisfies their business requirements.

Inappropriate classification of change can lead to inappropriate authorization of the changes to business information which can lead to fraud and irregularities. Without business owners confirmation to the live implementation of the change, there is a risk that the implemented change might not satisfy their business requirement.

I recommend management of TIB Development bank limited to establish system change forms which indicate the type of change and specifies the approval requirement of the specify change. I also recommend the management to ensure that the business owners review the live implementation of the change to confirm if the change meets their business requirements.

Correspondingly, my review of access rights to LGAs IFMS Epicor system noted that the security manager group has access to change configuration settings. Such settings were: Fiscal calendar, defining of prefix of legal number, restarting of processes in BPM, end of year closures to stop previous year's transactions, setting of new activity codes and accounts, system account categories which define assets and liabilities.

However, there were no formal approval procedures and testing for changes of settings in the system, this would ensure changes are authorized and do not affect reliability of the system which can cause instability. It was further noted that PO-RALG does not have a formal operational systems and application software change management procedures to control all changes of the systems. Uncontrolled changes to the system such as changes of configuration settings may lead to unauthorized changes and system disruption

I recommend management of PO-RALG to establish formal documented change management procedures and ensure changes of system configuration settings are subjected to formal change management controls.

CHAPTER THREE

3 EFFICIENCY OF INFORMATION SYSTEMS

This chapter summarizes issues relating to information systems' efficiencies. Specifically focusing on how information systems are operated and used by the government entities to attain the intended goal. The following are the noted deficiencies.

3.1 Operations not performed within the Systems

3.1.1 Non-compliance with IPSAS of LGAs IFMS Epicor system

URT adopted International Public-Sector Accounting Standards from 1 July 2004, both for local and central government. All reporting entities in the public sector have to apply IPSAS-based accrual accounting. Local government effectively started producing accrual-based IPSAS financial statements from 30 June 2008 on five years grace period ended on 30th June 2012 where all LGAs adopted full IPSAS compliance.

LGAs IMFS Epicor accounting system is not used to record accurately Accounts payable liabilities. The current commitment control setup checks availability of cash book balances before allowing payment to go through. The system also checks for funds balance in the selected line items in addition to the budget balance. The commitment control requires the availability of actual cash balances in the physical bank accounts before it allows transaction to go through contrary to IPSAS accrual, which requires recognition of expenditure when incurred and not when cash is paid. I further noted that users of the system are unable to enter creditor's records because the system requires funds to be available in the system cashbooks contrary to IPSAS accrual standard.

I recommend management of PO-RALG to carry out IFMS Epicor system customizations and enhancements to facilitate proper recording and reporting of IPSAS compliant accrual transactions.

3.1.2 Inconsistency between accounting manuals and accounting systems

My review of the Local Authority Accounting Manual (LAAM) noted that the manual implements the law, which demands uniform accounting system for all the LGAs, it also serves as a handy working document for those involved in the management and accounting of the Local Authorities' resources. The procedures, documents and books described in LAAM are the guidelines for the management of Local Government Authorities finances. All officials vested with such duties must strictly adhere to them in the performance of their duties. Therefore, LGAs IFMS Epicor system should be customized based on LAAM.

However I noted inconsistences of accounting procedures between LAAM and IFMS Epicor system. Identified inconsistencies include the use of cheque in making payments which is still specified in the LAAM while LGAs IFMS Epicor system is using electronic fund transfer for making payments, also according to LAAM payment should be approved by head of departments while currently in IFMS Epicor payments are approved by district/council treasurer.

I noted the same concern in my review of the TBS accounting Procedures Manual which was outdated and was not aligned with procedures implemented in the accounting software and Electronic payment system used by TBS.

This is attributed to lack of coordination between owner of accounting systems i.e chief accountant or finance director and ICT units as custodians of systems. I am concerned that these inconsistences can lead to missing controls or mandates in the accounting system, accounting manuals stipulate internal controls and mandates which should be customized in the accounting system.

I recommend management of PO-RALG and TBS to update the Accounting Manual to reflect the current laws, regulations and international standards also to ensure future changes in Accounting systems are first updated in accounting manual before being implemented in accounting systems

3.1.3 Accounting officers approve outside application systems

My review of voucher creation and approval for both PO and Non-PO voucher in LGAs IFMS Epicor and accounting systems of PAs noted that Accounting officers do not approve payments inside the accounting systems, instead approval is done on physical payment voucher printed from the system then treasurer or chief accountant approves inside the system.

My review of application access control of Muhimbili National Hospital (MNH) hospital information system noted that approval of canceling bills and charging patient's category are done outside the system using special form then afterward cancellation and changes are updated in the system. Review of sample of 19 canceled bills and 24 cases of changed patient's category from the system between 1st July 2017 and 30th June 2018 revealed that all 19 canceled bills had no signed approval form and 14 out of 24 cases had no approval to change category.

I also reviewed access controls of TFDA's Management Information System (MIS) and noted that certificates of registration are only issued from the system after getting the approval of the Director General and processing in the system. Thus final approval by the Director General of registration certificate was not done inside the MIS system which eliminates audit trail and accountability inside the system.

This is attributed by the fact that information systems have not been designed to allow AOs to approve inside the systems. Failure to approve inside systems eliminates accountability of accounting officers and audit trail in the systems. Also there is a possibility of making changes inside the system without AO's awareness leading to unauthorized approvals.

I recommend management of PO-PSM, MNH and TFDA to ensure approvals of accounting officers are also done inside the systems in parallel with manual approval done on printed documents. Accounting officers and all other signatories should login to systems to approve.

3.1.4 Exited transit goods not validated in TANCIS system

Part 5.5 of CED-706-F of Customs and Excise Department Transit Monitoring procedures require the Transit Monitoring Unit (TMU) officer at Head Quarter on daily basis to view the TANCIS system and establish all transit transactions which have remained invalidated after the statutory period.

My audit review of TANCIS data for transit goods (Dry and Wet cargo) at Kabanga, Rusumo, Mutukula, Tunduma and Kasumulu borders noted 599 transactions (entries) which were not confirmed to exit the country in the TANCIS system. However, our review of transit documents and manual registers maintained at the respective borders, indicated that the goods physically exited the country, but were not validated in the TANCIS system due to various control weaknesses, as summarized below

(i) Get out procedures were not performed in the system by customs officers at the departure gate at the Port in Dar es Salaam for 286 transit cargos (transactions). Therefore, this prevented the officers at the borders to perform the validation procedure; however goods were allowed to exit the country.

(ii) 70 transit cargos (transactions) were exited through wrong exit border. This happened whereby goods were physically transited and exited through borders different from the border indicated in the system.

(iii) 2 transit cargos were localized at TRA Customs head office, but were not updated in the system.

I am of the view that nonperformance of get out procedure in the system implies that goods were not permitted to depart at the port, and therefore were not supposed to be allowed to exit the borders. Moreover, exit of transit goods through wrong or different borders implies inadequate controls and monitoring of transit goods which may lead to diversion of transit goods into home use without payment of taxes. None updating of information in the system can mislead users.

I recommend management of TRA to

(a) Investigate the reasons for nonperformance of get out procedures at the departure port and ensure procedures are performed in TANCIS system.

(b) Ensure that all information in TANCIS system is timely updated and corrected to reflect the actual/real situation of respective transit cargos.

3.2 Government visibility over transactions

3.2.1 Visibility of actual collection by UDART via electronic payment cards not assured

DART entered into contract with UDART on 24th April 2015 for provision of passenger bus service, automated fare collection and integrated transport services system. In 2015 due to challenges existed on vendor's side in managing collections at bus stops the government decided to take over collection of fare by introducing LGRCIS system to replace vendor's system. However, the software used for fare collection through electronic payment card is still managed by vendor.

During the audit it was noted that DART's accountants have access to dashboard of the system which is used to collect electronic payment of bus fare. I am concern that the dashboard can be configured in favor of vendor to only show what vendor wishes DART to see. There is no mechanism for DART to get assurance on the integrity of transactions displayed on the dashboard.

I am of the view that lack of assurance on actual collection through electronic payment cards prevents DART from establishing actual collections for decision making

I recommend management of DART to have a fare collection system owned, hosted and managed by DART for electronic payments

3.2.2 Inadequate visibility of 1.1% deductions by mobile network providers from GePG payment transactions

Permanent Secretary, Ministry of Finance and Planning entered into contract with mobile network operators for Facilitating Integration to Government Electronic Payment Gateway at a price of 1.1% (One point One Percent Only), which will be charged from each payment transaction made by the customer with a condition that Government Revenue collected will be remitted to the Bank of Tanzania within Twenty Four (24) hours as per Terms.

My interview with GEPG team I inquired about the mechanism in place to ensure mobile network providers adhered to deduction of 1.1% of transaction; I was informed that surprise checks are conducted once in a while. Surprise checks are not sufficient and effective, mobile network operators should be monitored on real time to ensure they do not raise the percentage of deduction above the agreed rate in the contract. This poses a risk of undetected increase in percentage of deduction which will affect the general public.

3.3 Assessment of reliability of systems

3.3.1 Inconvenient billing systems for collecting government revenue

During my audit of Government Electronic Payment System (GePG) I noted that one of the limitation of effective collection of revenue is the inconvenience of billing systems of SP (government entities), most customers fail to pay because of difficulties in obtaining bills and control number from SP. Most of the billing systems of SPs are neither convenient nor user friendly which leads to loss of revenue since customers find it difficult to pay especially for those collections which lack enforcement or depends on discretion of customer.

Inconveniences of billing systems which were noted include; system unavailability, difficulties in generating bills especially for those online system which customers have to generate bills themselves, failures of systems to provide control number, ineffective mechanism to receive and handle reported complaints and failure to generate control number for bulk payments.

Among examples of inconveniences which were observed during the audit was the billing system of the National Board of Accountants and Auditors, the system does not allow to generate new control number after expiration of previous one thus if a member fails to pay within the timeframe he cannot regenerate a new control number, also it takes time to request control number due to system timeout attributed to either a system bug or downtime of the billing system and it does not have option for generating one control number for bulk payment of annual fee for members whose fees are paid by their employers.

Another case of inconvenience was noted in collection of traffic offense fees whereby the payment notifications do not contain control number which requires the offender to physically visit nearest police station to obtain control number. This is due to inadequate follow up and assessment of billing systems of SP in ensuring they are convenient for customers.

Such Inconveniencies can lead to untimely collection of revenue and in some cases revenues may not collected. Also they damage reputation and confidence of general public to the GEPG system.

I recommend management of MoFP to ensure that:

- GePEG team oversees development of billing systems and review revenue collection business processes of SPs to ensure they are user friendly and convenient in facilitating payments;
- SPs have effective mechanism to receive, record and handle complaints and support requests submitted by customers; and
- in collaboration with e-government agency develop guidelines on how to design and develop billing system to ensure standardization, convenience, security and availability.
- Government should standardize format of bills to include instructions on how customer can pay the bill and ensure each bill has control number

CHAPTER FOUR

4 MANAGEMENT OF ICT SYSTEMS AND PROJECTS

This chapter presents findings on the assessment of how IT projects are managed to realize value for money on the investment made. The following are the noted weaknesses.

4.1 Duplication of Efforts in implementing ICT Systems

4.1.1 HCMIS Lawson and GSPP

The Government salary payment platform system (GSPP) is the system developed under the Ministry of Finance through Department of Policy and Planning. The system has been established as validation of controls for the information submitted from HCIMS and crosschecking the same from the employers (Votes, councils, agency and other public institutions) on the actual figures of Wages and Salaries which are supposed to be paid to employees. The GSPP performs the same payroll validation as HCMIS system does. This implies duplication of efforts within government ministries. HCIMS could have been enhanced to save costs instead of developing a new application to manage payroll.

4.1.2 Online registration of class B business license

National Business Portal is among the National Projects implemented under Regional Communication Infrastructure Program (RCIP-Tanzania) through President's Office Public Service Management (PO-PSM). The Contract agreement was made on 1st September 2015 between President's Office Public Service Management and MFI Documents Solution Limited in respect of System Design, Development, Configuration, supply and Commission of the Design and Hardware for the Tanzania National Business Portal. The implementer of the project was Ministry of Industry and trade but later the project was transferred to BRELA.

My audit of the project revealed that in 2015 when the project implementation started one of the core requirement of the system to be developed was to enable registration of class A and B licenses, however class B licenses are issued by Local Government Authorities (LGA) and by then there was already a system (LGRCIS) acquired by

PO-RALG which accommodates this requirement. Ministry of Industry and Trade which was implementer of the project initially did not consult PO-RALG to avoid duplication of efforts. This was realized later after noticing the need to implement electronic payment for class B license, it was decided to integrate national business portal with LGRCIS. I am concerned that cost of the project could have been saved if there was a co-ordination efforts with PO-RALG at early stages of the project.

4.1.3 Salary slip portal

The ministry of finance and planning (MoFP) has developed an online portal for employees to access and print their salary slips. The same functionality is available in the Watumishi portal developed by PO-PSM. I believe efforts could have been coordinated to have one salary slip portal to save cost and time in managing two applications which serve the same purpose.

I am of the view that this is caused by lack of coordinated efforts among government institutions. I believe e-government Agency plays a role in ensuring there are no duplicate systems.

I recommend management of PO-PSM, MoFP and PO-RALG in collaboration with e-government agency to establish mechanism to strengthen controls to ensure efforts are coordinated to avoid duplication of ICT systems.

4.2 *Systems underutilization*

4.2.1 Unutilized procurement functionalities in LGAs IFMS Epicor

During My review of LGAs IFMS Epicor system specifically under purchasing and Purchase order receipts I noted that system has functionality that allows quality inspections / approval for goods received before they are paid for. However, I noted it is not used although it is very important to be used to assess the quality and quantity of goods received. On inquiry, Management explained that the inspection is done manually outside IFMS Epicor system by the stores department and by the personnel involved in the vendor selection to ensure that the goods meet the quality specifications.

My further review of implementation of procurement process in the system noted the availability of functionality in IFMS Epicor system which is aligned with the requirement under Sect164.-(1-6) of procurement Act of 2011 and its regulation 2013, 2016.

However the functionality has not been used for managing procurement process instead operations were done outside the system. The following were functionalities which have not been used while processing procurement contracts in the system; Creation and approval of requisitions, functionality which enable quotations to be obtained from at least three competitive suppliers, creation of Request For Quotation (RFQ) and entering of Line items and commitment of purchase order.

4.2.2 Unutilized asset module in LGAs IFMS Epicor

I also reviewed maintenance of assets records in the LGAs IFMS Epicor and revealed that LGAs do not maintain Assets records in IFMS Epicor system despite the availability of a fully licensed assets management Module in Epicor system. I further reviewed if the system is able to record assets and confirmed that is was possible to keep and record assets purchased and disposed by councils. The same weaknesses were also noted at EWURA and BRELA during my review of their IFMS Epicor accounting system, the system was fully licensed with capability to keep records of assets but the asset module has not been used.

4.2.3 Unutilized EDAMS modules in DAWASCO

My review of the DAWASCO Engineering Design Analysis Management System (EDAMS) noted that the system has five modules named Billing and Customer information, Network Asset management, Commercial Data Analysis/Commercial Data Validation (CDA/CDV), Demand Management, Operations and Maintenance. However, DAWASCO was using the first three modules only, on inquiry I was informed that utilization of these two modules depend on the availability of information in the network asset management module. If the entire network with all its components have been captured in the network asset management then the two modules can be used. I was further informed that there is a team under head of ICT unit which has the responsibility to ensure the entire network is captured in the network asset management module. However there was no plan and timeline for the team to complete the task while the network is expanding and

demands for maintenance continue to emerge. I am concerned that due to non-utilization of these two modules the corporation will fail to identify water supplied to detect water loss and plan for line maintenance without water loss, as a result can lead to failure to reduce non-revenue water.

I am of the view that the government cannot realize value for money for the functionalities which have been licensed but not utilized. Moreover, I believe use of system functions reduces human errors and increases efficiency as opposed to performing such functions outside the system.

I recommend management of PO-RALG, EWURA, BRELA and DWASCO to ensure they fully utilize functionalities of systems to realize value for money and improve efficiency.

4.2.4 Jeeva application underutilized in radiology department

Jeeva is an application acquired to improve effectiveness in managing business process and maintenance of medical records at MNH. With this application departments are supposed to operate paperless by fully utilizing functionalities available in Jeeva application to provide services.

I reviewed operations of the Radiology Department to establish whether services are provided as per client service charter. It was noted that the Radiology Department is not using Jeeva fully because requests for tests from doctors miss clinic notes which describes in details the test to be conducted. Jeeva has an option for entering clinical notes however doctors are not filling the notes; as a result Radiology Department requests for paper based clinical notes.

I am concerned failure to utilize the available system functionality can lead to difficulties in monitoring performance of the Radiology Department to ensure client service charter is adhered. Moreover, MNH cannot realize value for money of Jeeva application and continue incur cost of printing clinical notes

I recommend management of MNH to change clinical notes filled to be mandatory before submitting test request so as to enforce users.

4.3 Inadequate risk management

4.3.1 Lack of periodic ICT risk assessment and tracking of identified risks

My review of ICT risk management activities at MNH noted that risk assessment was last performed in 2014. ICT environment and risk universe has changed since 2014 as new application systems and technology have been acquired. Recommended practice is to conduct risk assessment at least once annually and whenever there are changes in ICT environment. Also, technology has changed together with introduction of new security risks. Therefore, risk assessment was supposed to be done to account for the changing ICT environment. Furthermore, my review of the risk assessment report noted that tracking of implementation of recommended mitigation strategies was not done, thus there was no assurance that identified risks have been mitigated.

4.3.2 Vulnerability assessment and maintenance of risk register not conducted

My audit of GePG system found out that since its rollout in July 2017 the system was formally assessed for security risks and vulnerabilities as required by section 4.3.9 of the GePG management framework. However, there was no effective mechanism in place to continue monitor vulnerabilities and implementation of recommended mitigations. GePG is a sensitive system which manages government moneys and it continues undergo enhancement, thus continuous monitoring of security risks is crucial. Further review of risk management revealed nonexistence of risk register to record identified risks associated with GePG system as required by section 5.5 of the GePG management framework.

According to my analysis, these weaknesses are caused by lack of information security officers to oversee the process of risk management. Inadequate risk management can lead to failure to detect vulnerabilities and security threats leading to non-confidentiality of information and non-availability of ICT resources.

I recommend management of MNH and MoFP (a) conduct ICT risk assessment at least once annually (b) maintain ICT risk register and monitor implementation of recommended mitigation strategy for the identified risks (c) consider having information security office to oversee what has been recommended in (a) and (b)

4.4 Inadequate ICT projects management

My audit of four ICT projects noted noncompliance with ICT projects management best practices and guidelines issued by e-government Agency guidebook for managing ICT project and risks. The following weaknesses were noted during the review of management of these projects:

4.4.1 Lack of project documentations

Section 2.6 of the e-government Agency guidebook for managing ICT project and risks outlined seven stages of ICT projects and required documentation as output of each stage. My review of project to upgrade LGAs IMFS Epicor system version 10.2 at PO-RALG found that project did not have the following vital documents; business case which outlines the justification for undertaking the project, requirements specification document which specifies what user expects the software or solution to be able to do and project plan to specify activities with duration and responsible person for easy monitoring.

Further review of project to acquire an online business registration portal at BRELA noted that the project had only document which is project plan while it was in final stages of completion. Documentations ensure standardization, enable future reference and provide assurance that best practices were adhered to.

4.4.2 Failure to transfer technology from vendors

Review of BRELA's project for design, development, configuration, supply and Commissioning of Software and Hardware for the Online Registration System revealed dependency on vendor in managing projects and failure to transfer knowledge to internal staff to be able to continue supporting the system after handover.

During the audit I noted that most of project documentations and clarification of concerns were provided by vendor rather than BRELA's project team who are the owner of the project. Moreover, continuity of support and future enhancement of the system was not certain due to failure to transfer knowledge to internal staff, as per contract the vendor Norway Registers Development (NRD) was to train ICT staff to be able to support and conduct future enhancement, however training was not conducted as expected.

According to my analysis, BRELA will continue to depend on vendor in supporting the system and implement future enhancement which is cost ineffective compared to using internal staff. I am of the view that non transfer of technology was caused by the use of system development technology which internal ICT staff were not conversant also vendor's inability to properly plan for technology transfer.

4.4.3 Ineffective project planning and monitoring

My audit of PO-RALG project to upgrade LGAs IFMS Epicor and BRELA's project for design, development, configuration, supply and Commissioning of Software and Hardware for the Online Registration System noted significant weaknesses in planning and monitoring of projects.

- **Non-monitoring of project expenditures**
  Audit of LGAs IFMS Epicor upgrade project found that project expenditures were not tracked thus it was difficult to establish total cost of project which formulates the cost of the system as an intangible asset in the asset register. Furthermore, failure to track project expenditure can lead to over payment to the vendor. This was observed in my audit of BRELA's Online

Registration System and business portal projects whereby vendors were paid for more than what was delivered.

- **Changes not implemented despite being within the warrant Period**
  During the audit of BRELA's Online Registration System project it was noted that two (2) change requests raised during user acceptance test were not implemented by the vendor during the period of free maintenance (warrant period) because BRELA failed to provide information which was required by vendor to enable the change request to be done.

- **Irregularities noted in conducting of user training**
  In my review of the project to upgrade LGAs IFMS Epicor I requested training manual, training plan and list of staff required to be trained and those who were trained. We were informed by the management that training was conducted to three accountants, one procurement officer and one human resource officer from each Council. However, the management could not substantiate by sharing training report and signed attendance of trainees thus I could not establish the number of staff who were trained and coverage of the training. Similarly my review of BRELA's Online Registration System project revealed that ICT staffs were to be trained for 28 days as per contract agreement but the training was conducted for three (3) days.

- **Weaknesses noted in conducting user acceptance test**
  During my audit of BRELA's Online Registration System project noted lack of evidence to substantiate testing of some of the design components of the system. Review of user acceptance test results and signoff report noted 9 components lacked test results and were not signed.

- **Fundamental Items not included in the contract and project plan**
  The contract and plan for BRELA's Online Registration System project and online business portal project did not require vendors to report about the unit test, integration test and

source code review conducted during development stage of system development process. Unit test, integration test and source code review are important aspects in identifying and fixing bugs prior to deploying the system for use.

According to my analysis, irregularities in managing ICT projects were attributed to lack of ICT projects office or project management personnel in government organizations which can ensure compliance with e-government guidebook for managing ICT projects and risks. If the government of URT is embarking on adopting ICT to improve operations and services then effective management of ICT projects is crucial. Inadequate management of ICT projects can contribute to failure to realize value for money and deliver intended objectives.

I recommend government of URT to (a) insist in establishing ICT project management offices in public organizations (b) e-government Agency to strengthen review of compliance with project management guidelines and best practices especially for big ICT projects (c) ensure internal staff can continue to support and maintain implemented systems after project completion

4.5 Inadequate ICT governance

4.5.1 ICT steering committee not formulated

My review of ICT governance noted cases of entities which did not have ICT steering committee to oversee ICT strategic planning as per section 2.3.4 of the e-government guidelines. For those entities which the committee existed it was not operational as per terms of references.

The audit of ICT governance at the GBT noted that the ICT steering committee was not formulated as required by section 2.3 of the GBT ICT policy. GBT was implementing a large project to automate its business process in collaboration with E-government agency and Ministry of Finance. I am therefore concerned that nonexistence of this committee can lead to failure of the project to deliver its intended objective due to lack of oversight and alignment with GBT strategic plan.

As per section 2.3.4.3 of the GBT ICT policy, one of the responsibilities of the committee is to monitor implementation status of major ICT projects, thus it is crucial for the committee to be in operation to monitor and manage projects, this will ensure the project will bring expected strategic value timely and in a cost effective manner. Management explained that responsibilities of the ICT committee were assumed by the management. However I believe ICT activities need special attention and prioritization given the role it plays in achieving organization strategic objectives, thus I am concerned that ICT cannot get the required level of attention in management meetings which underscores the need for a separate committee.

I recommend management of GBT to formulate the ICT steering committee, establish its terms of reference and ensure it operates as per its terms of reference.

TASAF established its ICT steering committee on 25th June 2014, review of the terms of references and operations of the committee noted terms of reference do not specify positions of members who are serving the committee instead it only states number of committee's members representing each of the functional areas of Operations, Failure to specify positions eliminates accountability.

Moreover, according to the terms of references the committee is to meet at least twice weekly (or as often as deemed necessary by the chair) but must meet monthly. It further requires regular minutes of the meetings to be circulated with decisions approved. However, review of the operations of the committee noted that it has not been meeting since its formulation. TASAF has been implementing strategic ICT projects which require oversight to ensure alignment with objectives and value for money, thus non-operation of the committee can lead to failure to realize return on investment in ICT.

I recommend management of TASAF to ensure the ICT steering committee is conducting its meetings as per terms of reference and minutes of meetings are maintained.

4.5.2 Ineffective reporting structure of ICT function

Paragraph 8.8 of the guideline issued in July 2012 by the President Office Public Service Management and Good Governance on the Appropriate, proper and safe use of ICT Systems outlines that ICT Section/Unit in Government Offices should report directly to the Chief Executive Officer (CEO) of the Entity. Moreover, according to section 5.3.2 of the E-Government Guidelines, Public Institutions shall establish an ICT Department/Directorate/Unit that reports directly to the Accounting Officer.

From My audit of GBT, I noted that ICT manager reports to the Director of Corporate Services thus ICT strategic needs and development must be channeled through Director of Corporate Services who reports to the Director General and Board for implementation. My review of ICT reporting structure of TFDA noted that ICT manager reports to the Director of Business Support.

I am of the view that ICT plays a critical role in every aspect of the organization operations in ensuring strategic objectives are achieved. Therefore, it is important that the ICT manager reports to the accounting officer whose major priority is the overall strategic performance of the organization.

I recommend management of GBT and TFDA to review their organization structure with the view to restructuring its Organization Structure for ICT Unit to report directly to the Director General.

4.6 Lack of internal information systems audit

Regulation 34(h) of Public Finance Regulations requires the Internal Audit Unit to review and report on the adequacy of controls built into computerized systems in place.

During my audit of LGAs IMFS Epicor I reviewed quarterly internal audit reports and noted that the Internal Audit Unit does not audit information systems controls. Further review of the minutes of meeting held by Audit Committee noted that the committee has not discussed matters relating to Information System Audit. I was informed

by the management that, the unit does not audit information systems because it lacks staff with knowledge on Information Systems Audit.

In the same way, the review of MNH internal audit function noted that the unit did not carry out full-fledged information system audits during the year under review. There was no evidence to substantiate that the systems have been audited in recent times except for few ICT related issues which were raised in the cause of normal financial audit. On inquiry I was informed that the unit does not have skilled personnel to review systems especially the backend activities done by ICT unit in administrating existing systems. Hence, management cannot get assurance on whether the IT internal and application controls are operating as desired.

I recommend management of PO-RALG and MNH to strengthen internal audit function to be able to conduct full-fledged information systems audits.

4.7 Inadequate IT general controls

4.7.1 Inadequate business continuity and disaster recovery plan

According to ISO/IEC 27002 Code of practice for information security management section 14.1.3 on developing and implementing continuity plans, plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes. Section 10.5.1 of the same standard requires Back-up copies of information and software to be taken and tested regularly in accordance with the agreed backup policy.

My review of business continuity and disaster recovery at PO-RALG found that the entity has no Business continuity plan which assesses business impact analysis and defines Recovery Point Objective (RPO) and Recovery Time Objective (RTO). This implies that there was no strategy to recognize potential threats and risks facing PO-RALG, to ensure that personnel and assets are protected and able to function in the event of a disaster.

I also noted that the DRP was not approved by the management to justify management's intent and expectations in ensuring continuity of information systems during disaster. My further review of information systems data backup procedures noted that PO-RALG has a mechanism to automatically copy backup of data and systems state to a secondary site every one hour. On inquiry about testing of of backup copies sent to recovery site, I was informed that testing of backup has been done by simulation however there was no evidence of report to substantiate.

Lack of BCP can lead to failure to resume the business in case of disaster due to non-identifications of key responsible people, key facilities in the resumptions, Contacts of key people, and non-awareness of people on what to do during the disaster. Also lack of defined RPO and RTO implies back up interval is neither appropriate nor agreed as per business impact, and business cannot resume within expected period.

I recommend management of PO-RALG to (a) Develop Business Continuity Plan (BCP) based on Business Impact Analysis and define RPO and RTO (b) Conduct DRP test and maintain test reports

My review of business continuity and disaster recovery procedures noted that PO-PSM has documented backup and recovery procedures however there was no business continuity plan (BCP) which determines backup and recovery strategies. BCP is an operation document which outlines management's expectations on continuity of operations; the plan defines critical applications together with their recovery time objective (RTO) and recovery point objectives (RPO), it also outlines disaster response and disaster recovery team with their responsibilities, disaster declaration and escalation procedures. Therefore without BCP the recovery and restoration procedures cannot suffice management's expectations in case of disaster.

Further review of Lawson backup procedure noted that there are daily backups and monthly backups however there is no consistency in doing backup and keeping records of backups which have been done, for example review of register of backup noted that for the year 2016

backups of September and October were not taken, also for the year 2017 only backup of April were recorded.

Moreover, copies of backup are maintained in external hard drives at the server room which subject them to the same disaster and risk as production data. Lastly during the audit it was revealed that periodic restoration test of backup copies were not being done to ensure that copies of backup can be restored in case of disaster.

I recommend management of PO-PSM to

(a) Establish documented business continuity plan and update Lawson recovery procedures as per BCP
(b) Strengthen controls to ensure consistence in taking backup of data as per schedule
(c) Periodic conduct backup restoration test
(d) Keep copies of backup in an offsite location far from the MoFP building where production server room is located

My other review of TBS procedures for backup of applications data noted that backup of Electronic Payment System (EPS) data is done using a script which is running daily at night and copy of backup is stored in the server located at the server room.

However, during the audit it was noted that the script was not working properly as on some of the days backup was not done. Storage of backup copies in the same premise of production poses a risk since in case of disaster both production and backup data can be affected. It was also revealed that backup of QualiMIS application is done on daily basis and stored in external hard drive. However, there was no evidence of consistency in performing backup on daily basis. Furthermore, backup copies of applications data have not been tested to ensure they can be recovered in case of disaster.

I recommend management of TBS to (a) ensure effective backup mechanism is in place so that daily backups are sent to recovery site (b) periodically test backup copies to ensure data can be recovered.

4.7.2 Lack of accountability and Nonexistence of MOU between government entities

Section 6.2 of the ISO/IEC 27002 International Standards Code of Practice for Information Security Management states that "where there is a business need for working with external parties that may require access to the organization's information and information processing facilities, or in obtaining or providing a product and service from or to an external party, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in an agreement or contract with the external party defining the terms and conditions for the connection or access and the working arrangement."

My review of implementation of LGRCIS system at DART for collection of bus fares and own source revenues at bus stops noted that the system was acquired, installed, hosted and managed by PO-RALG. However, there was no agreement or contract between DART and PO-RALG to define responsibilities and accountability of both parties. However, absence of formal contract or agreement hinders DART to hold PO-RALG responsible for any failure to meet operation expectations. Also matters such as disaster recovery plan cannot be certainly determined whether PO-RALG has designed recovery strategies which are aligned with DART's business continuity expectations.

Moreover, without MOU PO-RALG is relieved from the accountability to ensure effective security and performance of the system, for example on 22nd June 2018 DART reported to PO-RALG regarding system unavailability however the problem was not resolved timely as promised by PO-RALG, thus I am concerned such issues could have been taken care of by agreement to enforce PO-RALG to meet expected service level. Further review of operations noted that there were change requests to enhance the system which DART submitted to PO-RALG for implementation. However, there was no formal mechanism to keep record and monitor implementation of change requests.

I recommend management OF DART to (a) establish MOU with PO-RALG to define responsibilities of both parties and working arrangement (b) include in the agreement formal mechanism to report, record and monitor system change requests (c) in the long run DART should consider to host and manage the system

In my audit of HCMIS Lawson system at PO-PSM I visited the server room where the system is hosted and interviewed the System Administrator. According to the agreement between Permanent Secretaries of MoFP and PO-PSM in September 2010 with regard to management and administration of HCMIS Lawson system the responsibility of managing infrastructure of the system was given to MoFP. However, my visit to the server room and interview with Lawson system administrator it was noted that there was a defect of backup tap reader but it could not be fixed timely since the contract for maintenance expired, this contract was entered between MoFP and contractor thus backup were not done for a period of four months.

In addition, training and test servers at the server room were not operating due to hard disk failure and because of expiration of maintenance contract these servers were not used for at least three months starting from April 2018 as a result no application changes were done and resources of production environment were reduced as this server was providing resources to production servers.

I am concerned that untimely resolution of infrastructure failures can lead to disruption of operations.

I recommend management of HCMIS Lawson infrastructure to be transferred to PO-PSM as the owner of the system for prompt and easy response to issues.

CHAPTER FIVE

5.0 GENERAL CONCLUSION AND RECOMMENDATIONS

The chapter presents a summary of general conclusions and recommendations on the identified weaknesses during audit of information systems. In line with Section 40 of the Public Audit Act No.11 of 2008, and Regulations 86 and 94 of the Public Audit Regulations of 2009 which require Accounting Officers to prepare responses on the CAG's audit recommendations and submit to the Paymaster General.

I identified a number of issues and weaknesses on IT internal controls, application controls, ICT governance, ICT project management, ICT risk management and IT general controls surrounding information systems that require managements' intervention and implementation for future improvement;

Presented below is the summary of general conclusions and recommendations for the audit of information systems in the financial year ended 30th June 2018.

5.1 General Conclusion

(i) Government institutions have been embarking on adopting ICT to facilitate effective operations and service delivery. However, information security aspects have not been considered during acquisitions and implementation of ICT systems and solutions. Information security controls which have been overlooked during implementations of systems include

- Internal controls specified in international standards, accounting/financial manuals, internal policies and SOPs have not been well thought through and taken into consideration during requirements gathering and designing of information systems/applications.
- Information security risk assessment is not done at each stage of development of information systems.
- Vulnerability assessment has not been done before deploying information systems for use especially for critical financial systems.

This can result to weaknesses in application and security controls of systems resulting to loopholes which can be misused.

(ii) Accounting officers have not been using implemented systems in approving important documents, requests and applications submitted to them. My review of accounting systems and application systems which facilitate management of core operations of MDAs, LGAs and PAs revealed that AOs approve on printed documents in manual files instead of approving both on paper and inside the system. Systems have not been designed to allow AOs to login and approve instead approvals in systems were entered by subordinate officer after approval of AO on paper. I encourage AOs to personally be approving inside systems and login to these systems to review what has done by subordinates to ensure that what has been approved manually on paper is reflected in the system and maintain audit trails inside the systems.

(iii) Lack of coordinated efforts among MDA and PAs in implementing information systems which cut across entities as a result it lead to duplication of efforts which is costing the government. For example there are two online salary portals which are used to by public servants to access and print their salary slip; one was developed by MoFP and the other by PO-PSM. Another example is the online business portal for issuing class B business license at LGA level which was developed by BRELA while it was already developed by PO-RALG as a module of LGRCIS.

(iv) Most of billing systems of MDAs and PAs which have been integrated with GePG system are not convenient in facilitating generation of bills and control numbers for customers (general public) to pay, thus the government is not collecting revenue timely and in some cases losing revenue.

(v) Weakness in managing ICT projects attributed by lack of project management office in government institutions. MDAs and PAs have been utilizing considerable large amount of funds in implementing ICT projects for the purpose of improving service delivery, however my review has noted that these project are not adequately managed to ensure value for money and attainment of intended objectives. This is attributed by lack of dedicated responsible personnel to manage and monitor projects.

(vi) Application systems integration has not been considered during implementation. Projects to acquire or implement application systems have not been taking into consideration the need for integrating with other related systems especially integration with accounting system. This will ensure consistency of information between application systems by avoiding manual transfer of data from one application system to the other which is subjected to human errors and time consuming.

(vii) Nonexistence of information security officer position in government institutions to oversee information systems security and assess security risks on annual basis. Adoption of ICT in facilitating operations introduces security risks to information processed by the implemented systems thus having information security officer will ensure organizations' information security controls are updated with changing technology and IT environment.

(viii) Implemented information systems have not been full utilized while cost has been incurred to acquire/develop them. For example asset module of the LGAs IFMS Epicor system has not been activated to be used for recording and managing assets

(ix) Internal audit functions of most of MDAs, LGAs and PAs have not been equipped with required skills to be able to conduct information systems audit.

(x) Lack of Business continuity and disaster recovery plans which poses risks of failure to timely resume operations with acceptable amount of data in case of disaster

(xi) Inadequate ICT governance and reporting structure of ICT units whereby organizations do not have ICT steering committee and for those which the committee exists it is not operational as per terms of references. ICT steering committee provides oversight to ensure ICT strategic plan is aligned with organization strategic objectives and ICT projects are effectively managed.

(xii) Failure to transfer technology to internal ICT staff from vendors to ensure application systems will continue to be supported and maintained in a cost effective manner.

5.2 General Recommendations

Finally, as per the mandate vested in me under Sect. 12 of Public Audit Act, No. 11 of 2008, I have made a number of recommendations to the accounting officers. It is my belief that, if these recommendations are implemented will contribute to improving the management of information systems to ensure its security and effectiveness. The recommendations include the following among others:

- Accounting officers to champion the use of ICT by ensuring they utilize implemented systems in their day to day operations
- Government institutions to strengthen controls in ensuring internal controls and information security controls are effectively considered during implementation of application systems
- MDAs and PAs to consider establishing information security office for managing security risks associated with adoption of ICT in their operations. This will also ensure smooth implementation of my recommendation above.
- E-government agency to effectively strengthen its operations to ensure there are no duplication of efforts in implementing information systems in the government. \
- Government to establish ICT project coordination office under E-government agency to ensure large ICT projects are effectively managed and monitored.
- Strengthen internal audit functions by equipping them with skills to be able to audit information systems
- GePG team in collaboration with e-government agency to oversee billing systems to ensure their effectiveness in facilitating payment of revenue.
- Government to establish gaps of integrations especially for major application systems
- Business Continuity Plan and Disaster Recovery Plan to be given priority in government institutions to ensure continuity of operation.

ANNEXURES

Annexure 1: Summary of Audit findings with their respective risk rating

S/No	Description	Risk Rating
A	**EFFECTIVENESS OF THE INFORMATION SYSTEMS**	
1	2.1.1 Control weakness noted in LGA's IFMS Epicor system	High
2	2.1.2 Control weakness noted in accounting and revenue collection systems of Public Authorities	High
3	2.1.3 Control weaknesses noted in GePG generic billing portal	High
4	2.2.1 Weaknesses of interface between LGAs IFMS Epicor and TISS	High
5	2.2.2 LGAs IFMS Epicor and Treasury Single Account not integrated	High
6	2.2.3 HCMIS Lawson with Ajira portal and IFMS Epicor not integrated	Medium
7	2.2.4 Accounting software and revenue collection systems not integrated	High
8	2.3.1 Existence of duplicate employees in HCMIS Lawson system	High
9	2.3.2 HCMIS Lawson system allows net salary less than allowable amount	Medium
10	2.3.3 Inadequate validation control over approval of actions in HCMIS Lawson	Medium
11	2.3.4 Nonfunctioning of Commitment Control in LGAs IFMS Epicor system	High
12	2.4.1 Privilege user accounts not monitored	High
13	2.4.2 Non review of user access rights	High

S/No	Description	Risk Rating
14	2.4.3 Lack of documented application role matrix	Medium
15	2.4.4 Inadequate application of change controls	Medium
B	**EFFICIENCY OF INFORMATION SYSTEMS**	
16	3.1.1 Non-compliance with IPSAS of LGAs IFMS Epicor system	High
17	3.1.2 Inconsistency between accounting manuals and accounting systems	Medium
18	3.1.3 Accounting officers approve outside application systems	High
19	3.1.4 Exited transit goods not validated in TANCIS system	High
20	3.2.1 Visibility of actual collection by UDART via electronic payment cards not assured	High
21	3.2.2 Inadequate visibility of 1.1% deductions by mobile network providers from GePG payment transactions	Medium
22	3.3.1 Inconvenient billing systems for collecting government revenue	High
C	**ASSESSMENT OF MANAGEMENT OF ICT SYSTEMS AND PROJECTS**	
23	4.1.1 Duplication of efforts: HCMIS Lawson and GSPP	Medium
24	4.1.2 Duplication of efforts: Online registration of class B business license	Medium
25	4.1.3 Duplication of efforts: Salary slip portal	Medium
26	4.2.1 Unutilized procurement functionalities in LGAs IFMS Epicor	High
27	4.2.2 Unutilized asset module in LGAs IFMS Epicor	High
28	4.2.3 Unutilized EDAMS modules in DAWASCO	High

S/No	Description	Risk Rating
29	4.2.4 MNH Jeeva application underutilized in radiology department	Medium
30	4.3.1 Lack of periodic ICT risk assessment and tracking of identified risks	High
31	4.3.2 Vulnerability assessment and maintenance of risk register not conducted	High
32	4.4.1 Lack of project documentations	Medium
33	4.4.2 Failure to transfer technology from vendors	High
34	4.4.3 Ineffective project planning and monitoring	Medium
35	4.5.1 ICT steering committee not formulated	Medium
36	4.5.2 Ineffective reporting structure of ICT function	Medium
37	4.6 Lack of internal information systems audit	Medium
38	4.7.1 Inadequate business continuity and disaster recovery plan	High
39	4.7.2 Lack of accountability and Nonexistence of MOU with third parties	Medium