རྒྱལ་གཞུང་རྩིས་ཞིབ་དབང་འཛིན།

ROYAL AUDIT AUTHORITY

རྒྱལ་གཞུང་དངུལ་ལས་དབང་འཛིན་ནང་ བརྡོན་འཕྲུལ་རིག་མ་ལུགས་ཚུའི་བརྡོན་འཕྲུལ་རིག་རྩིས་ཞིབ་སྐོན་ཞུ།

IT Audit Report on IT Systems in RMA

སྤྱི་ལོ་༢༠༡༩ སྤྱི་ཟླ་༡༠ ཚ།

October 2019

Reporting on Economy, Efficiency & Effectiveness in the use of Public Resources

DISCLAIMER NOTE

The audit was conducted in accordance with the International Standards of Supreme Audit Institutions (ISSAIs). The review was confined to Integrated Central Banking System (ICBS), Indian Rupee and Convertible Currency (INR & CC) System, Authorised Money Changer (AMC) System in Royal Monetary Authority. The audit was based on the audit objectives and criteria determined in the audit plan and programme prepared by the Royal Audit Authority and the findings are based on the information and data made available by the Royal Monetary Authority.

This is also to certify that the auditors during the audit had neither yielded to pressure, nor dispensed any favour or resorted to any unethical means that would be considered as violation of the Royal Audit Authority's Oath of Good Conduct, Ethics and Secrecy.

རྒྱལ་གཞུང་རྩིས་ཞིབ་དབང་འཛིན།
ROYAL AUDIT AUTHORITY
Bhutan Integrity House
Reporting on Economy, Efficiency & Effectiveness in the use of Public Resources

RAA/TAD/RMA-ITA/2019-20/2579 **Date: 28th October 2019**

The Governor
Royal Monetary Authority
Thimphu

Subject: IT Audit Report of IT Systems in Royal Monetary Authority (RMA)

Dear Dasho,

Enclosed herewith please find the **IT Audit Report on 'IT Systems in RMA'** covering the period 1 January 2018 to 31 December 2018. The Royal Audit Authority (RAA) conducted the audit in line with the mandate enshrined in the Constitution of Kingdom of Bhutan and Audit Act of Bhutan 2018. The audit is conducted in accordance with International Standards of Supreme Audit Institutions on IT Audit (ISSAI 5300). The audit is also conducted in the context of Performance Auditing following the RAA's Performance Audit Guidelines, which is consistent with the International Standards of Supreme Audit Institutions on performance auditing (ISSAI 3000).

The overall audit objective was to determine the efficiency and effectiveness of Integrated Central Banking system (ICBS), Indian Rupee and Convertible currencies system (INR & CC) and Authorized Money Changer (AMC) systems in RMA. In order to achieve the overall objective, two sub-objectives were drawn; to assess whether IT based system deliver the operations of RMA efficiency and effectively and to ascertain the adequacy of general and application controls in the IT systems.

The report has been prepared based on the review of available documents, analysis of data, and discussion with relevant officials of the RMA. The report contains positive initiatives, shortcomings and deficiencies as well as recommendations aimed at improving the system.

The draft report was issued on 16 September 2019 to the RMA for factual confirmation, comments and feedbacks. Responses received have been incorporated as well as provided in the report as **Annexure 1**.

In line with section 55(16) of the Audit Act of Bhutan 2018, the audited agencies are required to fix the accountability. Therefore, we would request the RMA to fix accountability and submit the Accountability Statement and Management Action Plan (Format attached) for implementation of each recommendation with definite timeframe **on or before 30 January 2020. In the event of**

non-submission of the same, the RAA shall fix the responsibility for implementation of the recommendations on the Head of the Agency.

The RAA will follow-up implementation of the recommendations based on the Management Action Plan and Accountability Statement. Failure to comply will result in taking appropriate actions, which may include suspending audit clearances to the official(s) accountable.

We take this opportunity to acknowledge the officials of RMA for rendering necessary co-operation and support which facilitated timely completion of the audit.

Yours sincerely,

(Tshering Kezang)
Auditor General of Bhutan

Copy to:

1. Hon'ble Lyonchhen, Royal Government of Bhutan, Thimphu;
2. Hon'ble Gyalpoi Zimpon, Office of Gyalpoi Zimpon, Thimphu;
3. Hon'ble Speaker, National Assembly of Bhutan, Thimphu;
4. Hon'ble Chairperson, National Council of Bhutan, Thimphu;
5. Hon'ble Opposition Leader, National Assembly of Bhutan, Thimphu;
6. Hon'ble Chairperson, Public Accounts Committee, National Assembly of Bhutan, Thimphu (enclosed five copies);
7. Executive Director, Department of Internal Audit, RMA;
8. Assistant Auditor General, Follow-up and Clearance Division, RAA;
9. Assistant Auditor General, Policy, Planning and Annual Audit Report Division, RAA;
10. Office copy; and
11. Guard file.

P.O. Box: 191 | Kawangjangsa | Thimphu | Bhutan |Tel: +975-2-322111/328729/328730/324961 | Fax: +975-2-323491
Website: www.bhutanaudit.gov.bt | Email: info@bhutanaudit.gov.bt and tkezang@bhutanaudit.gov.bt

IT Audit Report on IT systems in RMA

MANAGEMENT ACTION PLAN REPORT

Recon No.	Audit Recommendation in brief	Action Taken or To be Taken	Estimated Implementation Date	Estimated Completion Date	Responsibility Entrusted to:	
					Name & Designation	EID no.
4.1	RMA should ensure that the IT systems developed are used for intended purpose					
4.2	RMA should institute robust IT controls in ICBS, INR & CC and AMC Systems					
4.3	RMA should institute mechanism to enhance management of Authorized Money Changers					
4.4	RMA should enforce proper segregation of duties					

ACCOUNTABILITY STATEMENT

IT AUDIT REPORT ON IT SYSTEMS IN RMA

No.	Recommendations	Personal Accountability		Supervisory Accountability	
		Name & Desig.	EID No.	Name & Desig.	EID No.
4.1	RMA should ensure that the IT systems developed are used for intended purpose				
4.2	RMA should institute robust IT controls in ICBS, INR & CC and AMC Systems				
4.3	RMA should institute mechanism to enhance management of Authorized Money Changers				
4.4	RMA should enforce proper segregation of duties				

(s/d)

TITLE SHEET

1.	Title of the Report	:	IT Audit of IT Systems in RMA
2.	AIN	:	16182
3.	Audited Entity	:	Royal Monetary Authority
4.	Audit Period	:	January 2018 to December 2018
5.	Audit Schedule	:	April 2019 to July 2019
6.	Audit Team	:	1. Kinley Zam, 200801105, Sr. Audit Officer
		:	2. Dhendup Tshering, 20140103380, Audit Officer
7.	Supervisor	:	1. Sonam Wangmo, 200401104, Asstt. Auditor General
		:	2. Sonam Delma, 200301048, Asstt. Auditor General
8.	Overall Supervisor	:	Chimi Dorji, 9610060, Deputy Auditor General

ACRONYMS AND ABBREVIATIONS

AASBB	Accounting and Auditing Standards Board of Bhutan
AIN	Audit Identification Number
AMC	Authorized Money Changer System
ATS	Annual Travel Scheme
BAS	Bhutanese Accounting Standards
BCP	Business Continuity Plan
BDBL	Bhutan Development Bank Limited
BoBL	Bank of Bhutan Limited
CAAT	Computerised Aided Auditing Tools
CC	Convertible Currencies
CCTV	Closed Circuit Television
DC	Data Centre
DPNB	Druk Punjab National Bank
DR Site	Disaster Recovery Site
DRP	Disaster Recovery Plan
GAAP	Generally Accepted Accounting Principles
GL	General Ledger
ICBS	Integrated Central Banking System
ICT	Information and Communication Technology
IDEA	Integrated Data Extraction and Analysis
IFRS	International Financial Reporting Standards
INR & CC	Indian Rupee (INR) and Online Convertible Currency (CC) regulatory data reporting system
ISSAI	International Standards of Supreme Audit Institutions
IT	Information Technology
MFIs	Micro Finance Institutions
RAA	Royal Audit Authority
REDCL	Rural Enterprise Development Corporation Limited
RMA	Royal Monetary Authority
SRS	Service Requirement Specification
USD	United States Dollar

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Royal Audit Authority (RAA) conducted the audit of "IT Systems in Royal Monetary Authority' as mandated by the Constitution of the Kingdom of Bhutan and Audit Act of Bhutan 2018. The audit is conducted in accordance with International Standards of Supreme Audit Institutions on IT audit (ISSAI 5300). The audit is also conducted in the context of performance audit following the RAA's Performance Audit Guidelines, which is in consistent with the International Standards of Supreme Audit Institutions on performance auditing (ISSAI 3000).

With the recommendation from statutory auditors of Royal Monetary Authority (RMA) on the need for conduct IT audit on the RMA's IT systems, the RMA had requested the Royal Audit Authority (RAA) to conduct an IT Audit vide letter no. RMA/IAD-09/2017-18/4093.

Recognising the role and mandate of RMA to ensure monetary stability in the country and the significance of IT systems in achieving this mandate and enhancing its operational efficiency, the RAA has carried out the IT audit of Integrated Central Banking System (ICBS), Indian Rupee and Online Convertible Currency (INR/CC) and Authorized Money Changer (AMC) covering the period 01 January 2018 to 31 December 2018.

The overall audit objective was to determine the efficiency and effectiveness of ICBS, INR & CC, and AMC systems in RMA. In order to achieve the overall objective, two sub-objectives were drawn:

- ✓ to assess whether IT based system deliver the operations of RMA efficiency and effectively; and
- ✓ to ascertain the adequacy of general and application controls in the IT systems under review.

During the course of audit, the RAA have noted that the implementation of ICBS, INR & CC and AMC has led to automating the functions of RMA. Apart from this, the following positive initiatives were noted:

i) Top management commitment towards IT initiatives;
ii) Established INR exchange counter in Phuentsholing which led to INR collection of Nu. 25 million as on 17 May 2019;
iii) Certified for PCI DSS (Payment Card Industry Data Security Standard) and ISO 27001:2013 (Information Security Management) in 2018;
iv) Issued directives to banking institutions regarding cybersecurity;
v) Developed and endorsed Information Security Policy in 2018;
vi) Existence of strong physical access security;
vii) Established the Disaster Recovery (DR) site using Bhutan Telecom's infrastructure.

Apart from positive achievements, the RAA also observed deficiencies and shortcomings. Some of the significant ones are summarized below:

i. The intended objectives of the IT systems under review were not achieved due to IT systems not being used optimally;
ii. Lapses in regulation of authorised money changers (AMCs) resulted in incomplete list

of AMCs, and discrepancies between the RMA and DoT list of AMCs. These have consequently impeded effective monitoring;

iii. Inadequacies in user access management had led to improper procedure for user account creation, weak password management, and access right were not updated for transferred officials;

iv. Weakness in application security were observed such as lack of session timeout in system, and unlimited unsuccessful logon attempts;

v. Inadequate input control in the system leading to acceptance of invalid data by INR & CC system;

vi. Lack of validation had resulted in duplicate data; and

vii. Improper segregation of incompatible duties in ICBS has led to poor access control.

These lapses were largely caused due to weaknesses in supervisory and monitoring controls which in turn had resulted in inefficient internal operations and impeded the regulation of foreign currencies.

Therefore, the RMA should seriously address these lapses and root causes in order to render the systems effective and credible. To address these lapses, the RAA have provided four recommendations:

a) RMA should ensure that the IT systems developed are used by intended purpose;

b) RMA should institute robust controls in ICBS, INR &CC and AMC systems;

c) RMA should institute mechanism to enhance management of Authorized Money Changers;

d) RMA should enforce proper segregation of duties.

The RAA hopes that RMA will make further improvements to the system, design and implement IT controls and mechanisms for efficient and effective business operations considering the time and effort spent to develop the IT systems.

CHAPTER 1: ABOUT THE AUDIT

1.1 Mandate

The Royal Audit Authority (RAA) conducted the "IT Audit of IT Systems in Royal Monetary Authority" as mandated by Article 25 of the Constitution of the Kingdom of Bhutan to audit and report on the economy, efficiency, and effectiveness in the use of public resources.

Further, Chapter 5, Section 69 of the Audit Act of Bhutan 2018 stipulates, "*The Authority shall carry out performance, financial, compliance, special audits and any other form of audits that the Auditor General may consider appropriate*."

1.2 Audit Standards

The RAA conducted this audit in accordance with the International Standards of Supreme Audit Institutions on IT Auditing (ISSAI 5300) and International Standards of Supreme Audit Institutions on Performance Auditing (ISSAI 3000). The RAA followed audit procedures as prescribed under RAA's Performance Audit Guidelines and IT audit manual to maintain uniformity and consistencies of approaches in auditing.

1.3 Audit Objectives

The overall audit objective was

- To determine the efficiency and effectiveness of Integrated Central Banking System (ICBS), Indian Rupee and Online Convertible Currency (INR & CC) and Authorized Money Changer (AMC) systems in RMA.

The sub-objectives were

1. To assess whether IT based system deliver the operations of RMA efficiency and effectively, and
2. To ascertain the adequacy of general and application controls in the systems.

1.4 Audit Approach Applied

Since the RMA has implemented the ICBS, INR & CC and AMC to cater to its operations, the appropriate audit approach was to use a combination of system oriented and result based approach. Through system oriented audit approach, the audit focused on IT management, IT controls and compliance to applicable rules. With the use of result oriented audit approach, the audit assessed the efficiency and effectiveness of IT systems in meeting the objectives of RMA.

The following researchable questions were derived from the combination of system oriented and result based approaches.

1. Has the system needs analysis been carried out?
2. Are the systems (ICBS, INR & CC, AMC) meeting the intended objective?

3. Has the IT based systems made the internal operations and regulation of convertible currencies efficient and effective?
4. Are the system users competent to use the system without hindrances?
5. IS there adequate supervision and monitoring for foreign exchange flows and AMCs?
6. Is there a policy developed and implemented for access control management in the systems?
7. Are there proper procedures in place for user account creation?
8. Are there proper procedures in place for password management?
9. Are there proper procedures in place for user account management?
10. Are the users given access rights based on their duties?
11. Are all input transactions accurate, complete and authorised?
12. Is there proper segregation of duties?
13. Has data processing been performed as intended and are all the transactions been processed as authorised, that no unauthorised transactions have been added?
14. Is the system protected to secure sensitive data against discovery and misuse and allow tracing from incident to underlying cause and back?
15. Is there business continuity plan and disaster recovery plan?
16. Are the reports (outputs) generated from the systems (ICBS, INR & CC, AMC):
    - ✓ Accurate and complete,
    - ✓ Reasonable in quantity and format,
    - ✓ Produced on time, and
    - ✓ Distributed to the right destination in a secure manner?
17. Are the reports generated from the systems used for effective decision making?

These researchable questions were used to conclude on the overall audit objective of determining the efficiency and effectiveness of ICBS, INR & CC and AMC systems implemented in RMA.

1.5 Audit Scope

Of the eleven IT systems implemented in RMA, three IT systems (ICBS, INR & CC and AMC) were selected for audit considering the criticality of the systems and its impact on achieving the overall mandate of the RMA to maintain stability and integrity of the country's financial system.

The ICBS is the biggest and the only system catering to most of the internal operations of RMA and is critical for functioning of the RMA, the INR & CC systems are used to regulate outflow of INR and other convertible currencies, and the AMC system is used to facilitate and regulate the exchange of foreign currencies without having to visit other commercial banks.

The other IT systems were excluded as one IT system, the Bhutan Financial Switch (BFS), is PCI DSS (Payment Card Industry Data Security Standard) and ISO 27001:2013 (Information

Security Standard) certified system, while the other IT systems were either insignificant or will be phased out or upgraded soon.

Thus, the audit examined the ICBS, INR & CC and AMC systems and business processes surrounding the systems. The audit covered general IT and application controls related to the system including operations, business continuity & disaster recovery. The data of these selected IT systems were examined and analysed from January 2018 to December 2018.

1.6 Audit Methodology

The RAA applied the following methodologies to gather information, analyze data and derive conclusions.

i. Examined RMA Act 2010, Foreign Exchange Rules and Regulations 2018, Foreign Exchange Operational Guidelines 2018, Reserve Management Policy, Currency Management Division Manual 2017, Guidelines for Operation of Currency Chest 2018, and Accounting Policy 2018;

ii. Reviewed system documents such as Information Security Policy 2018, Service Requirement Specification (SRS) of ICBS, system details of INR & CC and AMC, system user manuals and any other document related to ICBS, INR & CC and AMC;

iii. Conducted walkthrough to observe and understand the activities performed in the IT systems and the control activities implemented in the IT systems;

iv. Consulted with relevant officials and understood the system process and workflows in the systems and drew process-flow and workflow diagrams for each of the systems;

v. Performed analysis of user access levels of different officials;

vi. Test checked and examined the input and validation controls implemented in the all three systems;

vii. Performed vulnerability assessment of INR & CC and AMC systems;

viii. Selective review of hard copy documents relating to transactions in the system to check the authenticity of the transactions in the systems;

ix. Analysed data in the IT systems using IDEA[1] to determine the integrity and accuracy of data, to assess the correctness of any calculations, and to ascertain the reliability of the reports generated;

x. Verified the reports generated by the IT systems and assessed the accuracy, completeness and reliability of the reports for effective decision-making;

xi. Interviewed all system users regarding system reliability, usability, issues and problems, and additional features needed in ICBS;

xii. Interviewed relevant officials from each Department to map each module of ICBS to the operations of the Departments in RMA;

xiii. Visited regional offices of Monggar and Phuentsholing, the extension counter in Phuentsholing and the counter for AMC in Paro International Airport to collect

[1] Interactive Data Extraction and Analysis (IDEA) is an auditing tool used by RAA for data analysis

information on their understanding of INR & CC and AMC systems and RMA's policies;

xiv. Visited commercial banks (BoB, Thimphu Main Branch and Phuentsholing Branch, Druk PNB, Tbank) to gain an understanding of how the CC system is being used in the banks and how the information and reports are being submitted to RMA;

xv. Visited authorised money changer agents in Thimphu to assess the usage of AMC system and the reporting mechanism between the AMC agents and RMA;

xvi. Visited Department of Trade to obtain the list of AMC agents license holders and performed a comparative analysis of licenses issued by DoT with RMA's list;

xvii. Visited the Disaster Recovery site in Phuentsholing and the Data Centre in Thimphu to determine the level of physical and environmental security controls implemented at these sites.

CHAPTER 2: INTRODUCTION

With the recommendation from statutory auditors of Royal Monetary Authority (RMA) on the need for conduct IT audit on the RMA's IT systems, the RMA had requested the Royal Audit Authority (RAA) to conduct an IT Audit vide letter no. RMA/IAD-09/2017-18/4093.

Recognising the role and mandate of RMA to ensure monetary stability in the country and the significance of IT systems in achieving this mandate and enhancing its operational efficiency, the RAA carried out the IT audit of ICBS, INR & CC, and AMC covering the period 01 January 2018 to 31 December 2018. Further, since these selected IT systems are critical systems for the functioning of RMA and for the regulation of foreign currencies, it is imperative to have adequate controls embedded in the systems to generate accurate and reliable information for decision making regarding the country's monetary policy.

2.1 Background on RMA

RMA as a central Bank of Bhutan has the mission of "*reinforcing stable and inclusive economic growth, maintaining stability and integrity of the financial system, advancing innovative services and technology*." The RMA plays a vital and unique role in the country's economy.

The Royal Monetary Authority of Bhutan acts as a banker, adviser and financial agent to the Royal Government. In this capacity, the RMA issues national currency, manages gold, reserves and foreign exchange operations, makes and oversee regulation covering payment and settlement systems. The RMA supervises and regulates Bhutan's financial institutions that comprise of five banking institutions and five non-bank financial institutions. Besides, new micro-financial institutions have also been established in the recent years. The RMA plays a vital role in promoting macroeconomic stability and economic growth in the country.

With huge mandate to ensure economic growth, price stability and monitoring the financial systems in the country, the RMA has undertaken several initiatives. Among such initiatives, the RMA has leveraged ICT and implemented eleven IT systems to enhance operational efficiency and effectiveness, and to improve service delivery. The eleven IT systems are as follows:

1. Integrated Central Banking system (ICBS),
2. Indian Rupee and Online Convertible Currency (INR & CC),
3. Authorized Money Changer (AMC),
4. Society for Worldwide Interbank Financial Telecommunication (SWIFT) system,
5. Druk Micro Fin system,
6. Remit Bhutan,
7. Cheque Truncation System,
8. Bhutan Financial Switch,
9. Bhutan Immediate Payment Service and Payment Gateway,
10. Central Registry Secured Transaction System, and

11. Electronic Fund Transfer and Clearing System

Out of these, three IT systems (ICBS, INR & CC and AMC) were selected for audit considering the criticality of the systems and its impact on achieving the overall mandate of the RMA to maintain stability and integrity of the country's financial system.

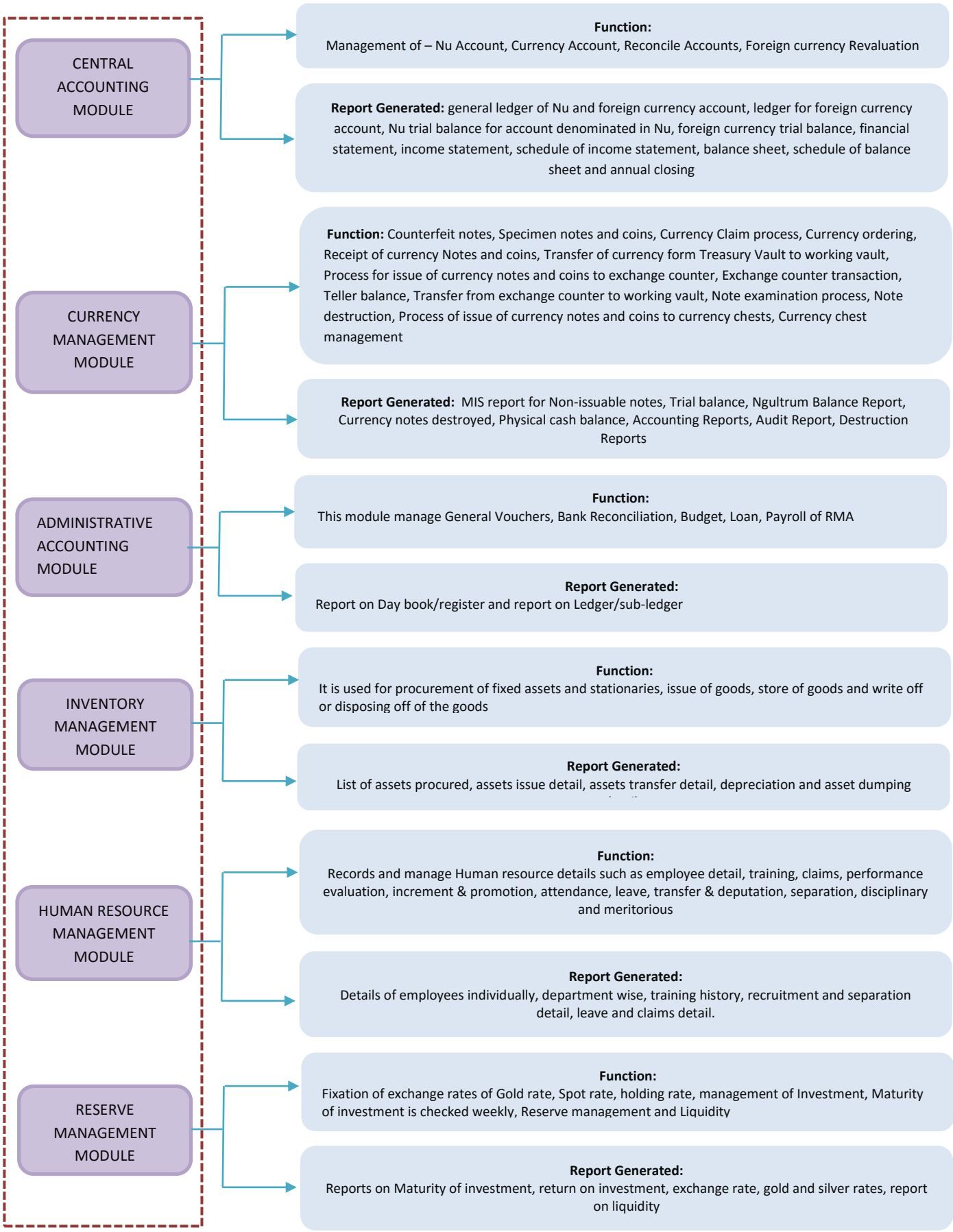
2.2 Integrated Central Banking system

ICBS is a centralized central banking solution which was developed in house to strengthen the RMA's institutional and functional capacity. It improves the efficiency as well as the quality of services it renders to the entire Financial System in the RMA and is therefore critical for the effective functioning of the RMA. It is however very important to note that the ICBS is a standalone system and not linked with any other systems in the RMA.

The ICBS software is developed on 3-Tier architecture which allows RMA greater flexibility by allowing them to work or update on a specific part of the architecture independently of others which improves speed of development, enhances scalability, and improves performance and availability.

The ICBS consists of the following 6 modules:

1. **Central Accounting Module (CAM)**
   CAM allows timely and efficient recording, computation and retrieval of accounting information by authorized users, managers and decision makers improving the central accounts operation capacity in RMA.
2. **Administrative Accounting Module (AAM)**
   AAM has interfaces with other modules such as HRMS, CAM, IMM and assists the RMA to keep track of all accounting details.
3. **Currency Management Module (CMM)**
   CMM allows the user to access to up-to-date information about the currency issue, receipt and other relevant processes.
4. **Inventory Management Module (IMM)**
   Inventory Management Module assists in record keeping, timely reporting and retrieving of inventory and asset related queries of RMA.
5. **Human Resource Management Module (HRMS)**
   HRMS is used to record and update personnel information and actions of RMA employees. In addition, it streamlines HR processes such as recruitment, hiring, promotion, transfer, leaves and separations.
6. **Reserve Management Module (RMM)**
   The RMM manages convertible currency and rupee reserve, monitoring the financial institutions and maintaining the exchange rates.



Process Flow in ICBS Figure 1: Business process flow of ICBS, prepared by RAA (Source: RMA)

2.3 Indian Rupee and Online Convertible Currency (INR & CC) system

The Indian Rupee and Online Convertible Currency (INR & CC) regulatory data reporting system captures all the CC and INR transactions from the commercial banks. Similarly, like the ICBS, this system was also developed in-house and by 2017, it was installed for operation. The system was also developed to provide complete data of the CC and INR transactions on a near to real time basis.

The system validates customer requisition on a real-time basis using CID as the unique key identifier. For instance, the system will provide alert messages and decline the application if the particular CID has already availed the annual quota of USD 3000 per person limit.

The system is a web-based application and the end user can access the system by providing secure login credentials.

Process Flow in INR

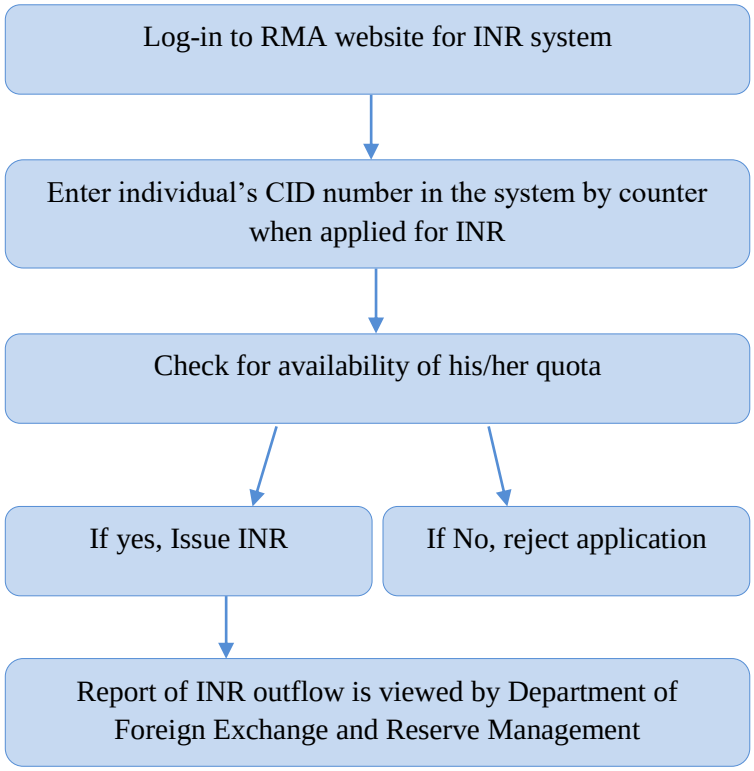


Figure 2: Business process flow of INR ATS in INR & CC system (Source: RMA)

Process Flow in CC

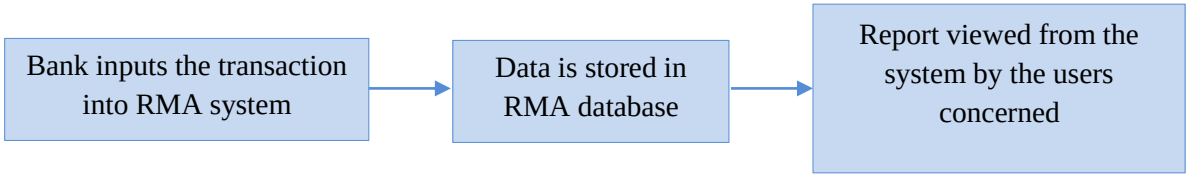


Figure 3: Business process flow for INR & CC system (Source: RMA)

List of report generated

- INR inflow and outflow report
- CC inflow and outflow report

2.4 AMC system

Authorised Money Changer system (AMC) was developed in-house to facilitate licensed agents in Bhutan to accept or buy permitted convertible currencies for exchange with Ngultrum. The system is linked with the database of the centralized ICBS and, retrieves and uses data from the ICBS system for functioning.

The system was first implemented by RMA in 2008 and then further upgraded in 2018.

AMC system process flow

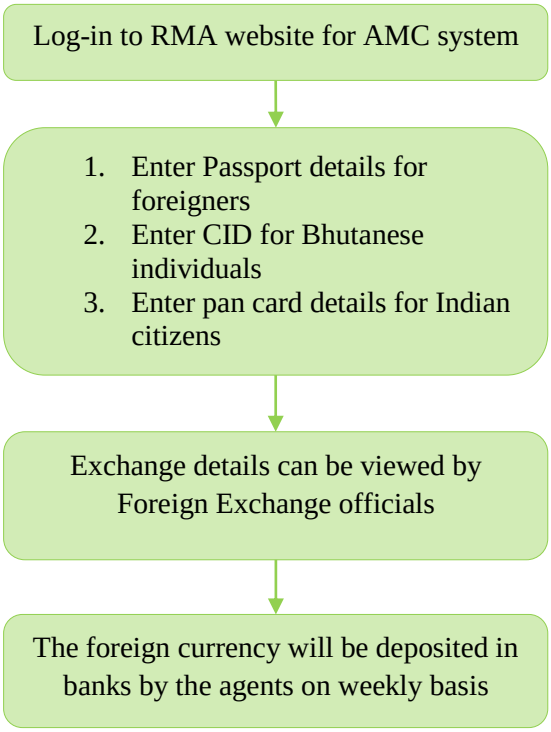


Figure 4: Business process flow for AMC system (Source: RMA)

List of report generated

- Transaction wise report
- Monthly consolidated report
- Daily consolidated report
- View exchange memo

CHAPTER 3: AUDIT FINDINGS

This chapter is divided into two parts: Part 1 highlights the positive initiatives and Part 2 discusses the shortcomings and deficiencies in ICBS, INR & CC and AMC in RMA.

Part 1: Initiatives and Positive Developments

The implementation of Integrated Central Banking System (ICBS) has automated the functions of RMA and resulted in capturing essential information of RMA's operations. Similarly, the Indian Rupee and Online Convertible Currency (INR & CC) system has made it easier to monitor the limits on foreign currencies for Annual Travel Scheme, and the Authorized Money Changer (AMC) has facilitated the exchange of foreign currencies through AMC agents.

Apart from the aforementioned positive developments, the RMA has undertaken several initiatives which had resulted in positive developments and the significant ones are summarised below:

i. Top management commitment towards IT initiatives.

ii. In order to regulate INR currency, and facilitate the exchange of INR into Ngultrum and exchange of unspent Ngultrum, the RMA had established an exchange counter at the Immigration Regional Office in Phuentsholing. The establishment of the exchange counter has led to INR collections of more than Nu. 25 million from its operation on August 2018 till 17 May 2019.

iii. To integrate with the RuPay Network of National Payment Council of India, the RMA was certified for PCI DSS (Payment Card Industry Data Security Standard) and ISO 27001:2013 (Information Security Management) in 2018. This was carried out to assess the Bhutan Financial Switch's ability to protect the card holders' data and connect with the National Financial Switch of India.

iv. In the wake cyber incident in some of the banks, the RMA had issued a directive to the banks on cybersecurity in April 2019 asking the banking institutions to implement basic IT security controls. The directive also instructed the banks to replace magnetic strip based cards with Europay Master Visa (EVM) chip and pin cards, and also upgrade the terminals (POS and ATMs) accordingly. Additionally, the RMA mandated the banks to work towards assessing PCI DSS aimed at protecting their Cardholder Data Environment and suggested the banks to certify for ISO 27001:2013.

v. The RMA have developed Information Security Policy in 2018 which was endorsed by the Information Security Committee chaired by the Deputy Governors.

vi. The RAA found that the physical access security to the RMA building is manned by security guards round the clock and access inside is logged with visitors log wherein the laptop details of the visitor is also captured. Further, physical access and environmental security to critical IT infrastructure were found to be adequate.

vii. The RMA has established the Disaster Recovery (DR) site using Bhutan Telecom's infrastructure.

Part 2: Shortcomings and deficiencies

While recognizing the positive contributions made after implementing the IT systems (ICBS, INR & CC and AMC), the RAA's review also revealed areas that require further improvements. The findings were made based on review of available system documents and analysis of data using Computerised Aided Auditing Tools (CAAT) i.e. Integrated Data Extraction and Analysis (IDEA).

3.1 The intended objectives of selected IT systems not achieved

The RMA is responsible for development of monetary policy that aims to keep the Ngultrum as stable as possible and maintain price stability in the country. To achieve its goals and objectives, the RMA recognised the potential of ICT as a key enabler in enhancing its operational efficiencies, and embarked on automating its business processes and developed relevant IT systems.

Any system development project is a huge commitment and a major undertaking with resources needed to develop and maintain it. Thus, it is imperative that the intended purpose and objectives of the system being developed is defined clearly at the onset itself. Business or functional requirements supporting work processes require integration across multiple functions and departments which need careful planning and identification of all business operations, common usage scenarios, and user workflows. Therefore, the IT system being developed should adequately support the RMA's business operations.

Similarly, it is equally important that users accept the IT system and use the system optimally to generate business value and value for money. In this regard, the RAA ascertained whether intended objectives of INR & CC, AMC and ICBS systems are achieved and whether the selected IT systems support the RMA in enhancing efficiency and effectiveness of its operations. During the assessment, the following were noted:

3.1.1 INR & CC system does not generate comprehensive INR and CC inflow and outflow report

The RMA is responsible to monitor the Convertible Currency (CC) and Indian Rupee (INR) outflow and inflow of the country and to provide real time information to the management for decision making. Accordingly, the INR & CC system was developed to support this function of RMA which is used by commercial banks and in RMA counters. The system is web based and designed to allow relevant Departments to view and monitor the transactions on a near to real time basis.

This system is designed to generate one of the most important reports of RMA; the INR inflow and outflow report and the CC inflow and outflow report. These reports are used to monitor the trade balance of the country. Since the reports generated are consumed to make

significant decisions regarding the country's economy; it is of paramount importance that INR & CC generates accurate and reliable information.

While reviewing the INR & CC system, the RAA noted that the INR & CC system does not support the intended functions. More specifically, the following were noted.

i. Although the INR & CC does have features to capture the required information, only the INR and CC transactions for Annual Travel Scheme (ATS) are captured fully while the transactions for other purposes are maintained in MS Excel (Microsoft Excel) manually.
ii. The RAA have visited all commercial banks in Thimphu to verify if the systems are used as intended. It was found that except for Druk Punjab National Bank, all other commercial banks are using the INR & CC system. However, the real time information is not fed into the INR & CC system. All the transactions are recorded in MS Excel and reported through mail on monthly basis to RMA. The intention of instituting online system to fetch and view real time transaction is not met.

As a result, the INR & CC system has not met the intended objectives and more importantly, do not generate comprehensive INR inflow and outflow report, and CC inflow and outflow report.

The INR and CC transactions for purposes other than ATS are maintained in MS Excel because the bank officials feel it is cumbersome as they have to enter in the same information firstly in their Core Banking System, then in a register, and also in MS Excel. Only when the bank officials get some free time – which is rare as they have to cater to clients – do they enter into the INR & CC system at a later date. The records maintained in MS Excel are submitted to the RMA as a compliance requirement as the RMA does not insist on the banks to use the INR & CC system.

The reports received by the RMA are consolidated by a dedicated official, which is then entered into the Executive Dashboard of RMA for top management. Such reports maintained in MS Excel come with inherent problems such as data integrity, delays in receiving the reports, inconsistencies in the reports, etc., which raises the question on reliability of the current compiled and consolidated INR and CC inflow and outflow report.

The INR & CC system has been in operation for more than three years, yet the processes of INR and CC transactions has become more cumbersome instead of being efficient. This indicates that the system is not meeting the intended objectives as it is not used to regulate the transactions on a near to real time basis nor does it generate comprehensive INR and CC inflow and outflow reports.

While accepting the issue in general, the RMA responded that it would remain the same until a 'proper solution' is implemented.

The RAA maintains the stance that the INR & CC system is not used for its intended purpose impeding real time monitoring of foreign exchange flows and entailing extra efforts to compile and consolidate the INR and CC inflow and outflow reports outside the system.

There is no need to integrate the INR & CC system with the Core Banking Systems of banks but ensure the use of INR & CC system by all the system users.

3.1.2 AMC system is not optimally utilised for regulation

Since exchange business has become lucrative, the illegal money exchange business is common all over the world affecting the overall economic stability of the country. In order to control illegal money exchange and to properly regulate the exchange foreign currencies, the RMA has initiated he Authorized Money Changers (AMCs) agents under the Foreign Exchange Rules and Regulation 2018 to deal in exchange of convertible currencies.

There are two types of AMC, one standalone whose license is issued based on trade license issued by the Department of Trade (DoT), Ministry of Economic Affair, specifically for the money changing business. The other one is the hotels wherein money changing license are issued based on the certification by Tourism Council of Bhutan as tourist hotels.

In order to facilitate money changing services, RMA has developed the AMC system to be used by all AMCs. The AMCs are supposed to record all foreign exchange transactions in the system for easy monitoring and effective regulation by RMA.

During the field visits to ten AMCs, the RAA found the following:

i. Only three AMCs were found using AMC System while the rest, seven AMCs, were not using the AMC system. Furthermore, upon the analysis of AMC December 2018 data, it was noted that only nine Hotels as shown in Table 1 have recorded their foreign exchange transactions in AMC system. Not using the system by AMCs will inhibit RMA to effectively regulate foreign currencies in the market.

Table 1: List of AMCs using AMC system in December 2018

Sl. No.	Authorised Money Changer	No of transactions
1	Hotel Norpheling	1
2	Tenzinling Resort	1
3	Zhiwaling	4
4	Olathang Hotel	6
5	Hotel Druk	6
6	Dhensa Boutique Resort	15
7	Le Meridien Thimphu	17
8	Taj Tashi	19
9	Le Meridien Paro Riverfront	22

The RMA reasoned that the AMC system was not used by most AMCs, leading to fewer transactions in AMC system, because

- **the payments for hotels are directly remitted to TCB;**
- **system compatibility issue of AMC system with the AMCs core system;**
- **trained AMC staff had left without training the successor.**

Further, the RMA assured to carry out ad-hoc inspections henceforth.

Since the RMA is already aware of the causes and having invested in developing the AMC system, the RMA should look into how the AMC system can be optimally utilised by the AMCs even without integration.

ii. The review of AMC system also revealed that the system does not maintain complete list of AMC license holders, which otherwise would have enabled the management in effective regulation and monitoring of foreign exchange transactions.

The RMA, in their response, mentioned that 'We have the updated list of AMC which we continue to update upon renewal of AMCs. We are in the process of reviewing the AMC application form and will be incorporating changes with applicant details where necessary. And as recommended we will host the updated lists on the RMA website and AMC online system for monitoring purpose. Therefore we would appreciate if the above observation can be dropped.'

The RAA verified the updated list provided and found that it was the same one given to the audit team before. The RAA would like to stress that the list is not maintained in the AMC system and the RMA should make provisions to capture complete list of AMCs in the system wherein the system can generate the list when needed for monitoring and reporting purposes.

iii. While reviewing the AMC system, the RAA found that the system does not have feature to assess AMCs' performances nor does it have records evidencing that RMA has assessed the AMCs' progress for monitoring purpose. Additionally, the Memorandum of Instruction (MoI) issued by RMA clearly states that license granted by the RMA is valid only for a year and shall be renewed based on the performance/operation of the business. Nonetheless, the RAA noted that the licenses for AMC are renewed even though the business remained inactive for more than two to three years.

The RMA, in their response, explained about the process of renewal of AMC license and iterated that the renewal will be based on performance of the AMC concerned.

The RAA acknowledges that the renewal of AMC license will be based on the performance. However, the RAA would like to clarify that the AMC system should have features to capture the performance of each AMC in order to document their performances and serve as a basis to renew their licenses in the future.

These lapses clearly show that AMC system was not optimally used as intended due to lack of adequate supervision and monitoring of these AMCs by RMA. Consequently, this had also resulted in ineffective regulation of AMCs.

3.1.3 ICBS does not support some core functions of RMA

The RMA developed the ICBS system and automated some of the core functions and internal operations of RMA such as banking, currency management, foreign exchange, reserve management, accounts & payroll, HR management and inventory.

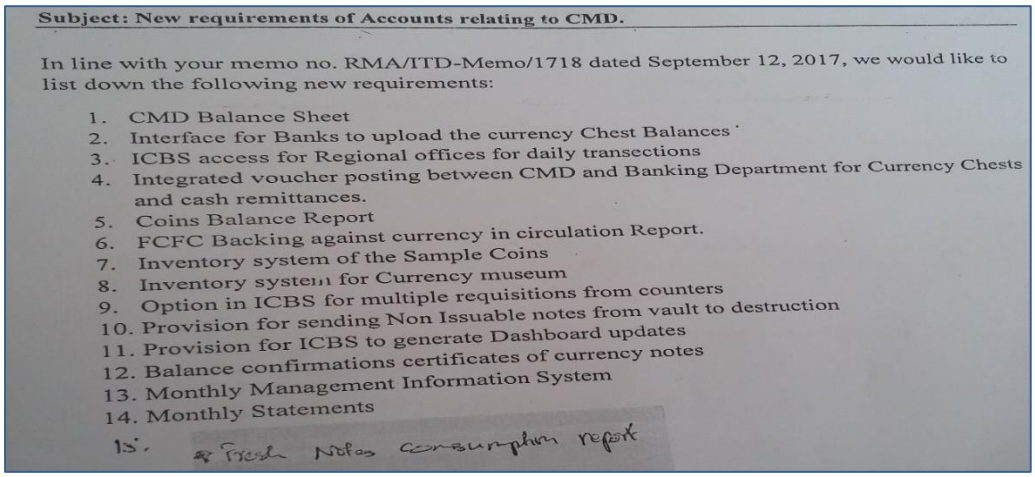
The ICBS should be able to support all the requirements and mandates of the organization to deliver services on time and manage resources efficiently. The system should always provide accurate information for decision making purposes. Thus, the system should be regularly upgraded and required changes must be incorporated with change in business processes.

Upon review, the RAA noted that the ICBS never underwent an upgradation or had enhancements since its development in 2007. Even though the policies, rules and standards of the organization witnessed numerous changes since 2007, no adjustments or enhancements were made to the system in order to support and meet the new requirements.

Due to which, the ICBS does not support BAS (Bhutan Accounting Standards) and IFRS (International Financial Reporting Standards) requirements for preparing financial statements. The RMA is in the process of complying with BAS as required by the Accounting and Auditing Standards Board of Bhutan (AASBB). However, the ICBS was developed mostly in compliance with the Generally Accepted Accounting Principal (GAAP) and was not enhanced to meet the requirements of BAS. The RAA noted that accounting and reporting tasks were carried out separately outside the system in MS Excel. Likewise, the ICBS does not support the reserve management functions.

Additionally, the RMA is also required to comply with International Financial Reporting Standards (IFRS) by end of 2022, which would bring further changes to the existing accounting system. In order to fulfil this requirement (to comply with IFRS), the Department of Banking has submitted the requirements to incorporate in ICBS to the management. According to the three-year strategic plan of Department of Banking, there is a requirement for robust accounting system which accommodate BAS and IFRS requirements.

Similarly, the Department of Currency Management had requested the following change requirements in ICBS as shown in Figure 5.



Subject: New requirements of Accounts relating to CMD.

In line with your memo no. RMA/ITD-Memo/1718 dated September 12, 2017, we would like to list down the following new requirements:

1. CMD Balance Sheet
2. Interface for Banks to upload the currency Chest Balances
3. ICBS access for Regional offices for daily transections
4. Integrated voucher posting between CMD and Banking Department for Currency Chests and cash remittances.
5. Coins Balance Report
6. FCFC Backing against currency in circulation Report.
7. Inventory system of the Sample Coins
8. Inventory system for Currency museum
9. Option in ICBS for multiple requisitions from counters
10. Provision for sending Non Issuable notes from vault to destruction
11. Provision for ICBS to generate Dashboard updates
12. Balance confirmations certificates of currency notes
13. Monthly Management Information System
14. Monthly Statements

15. Fresh Notes consumption report

Figure 5: Change request for ICBS

These changes were not incorporated till date and subsequently, the ICBS does not cater to some core functions such as generating the financial statements of the RMA. Not enhancing a critical system such as ICBS might lead to the system becoming redundant and not being used for their business operations.

The RMA responded that 'ICBS system consists of different integrated modules, such as HR, Inventory, Currency and Banking, etc. The system has been enhanced over time, based on the change request, which are mostly related to changes in the accounting policy from GAAP to IFRS. The implementation is still under the transition stage and is expected to be fully compliant by 2022. Till date, the accounting conversion and the related financial reporting were developed compliant with IFRS. Given that the accounting conversion is an ongoing process, requiring new requirements and scope to be finalized by the business owners, the existing system will be further enhanced to support new accounting policy. Therefore we would appreciate if the observation can be dropped.'

As assured, the RMA should ensure that relevant changes be incorporated and implemented in ICBS system with the change in business requirements.

3.2 Lapses in regulation of Authorised Money Changers

The RMA, being the central bank of Bhutan, has the authority to issue, renew and revoke the licenses of Authorized Money Changers (AMCs). The RMA is also mandated to monitor the function of AMCs on periodic basis to ensure that the functioning of AMC is in compliance with the Memorandum of Instruction (MoI) and the Foreign Exchange Rules and Regulation 2018.

In Bhutan, the RMA has started allowing authorized money exchanging business since 2012 and as of August 2019 there are 58 authorized money changers including Hotels and Standalone in the country according to the list maintained by RMA and the list of trade license holders for foreign exchange business obtained from the DoT.

In absence of complete list of AMCs from the system, the RAA obtained the manual list from RMA as well as from DoT for comparison and analysis.

3.2.1 Discrepancies between the RMA and DoT list of AMCs

The RAA reviewed and compared list of AMCs licensed by RMA as well as the list obtained from DoT and noted the following discrepancies:

i. ***AMC license issued by RMA but not registered with DoT for trade license***
   As per MoI for AMCs, RMA shall issue license for AMCs only on producing valid trade from DoT. However, upon the comparison of list of Standalone AMCs, it was noted that there are 16 standalone Money Changers and out of 16 AMCs, five had obtained license from RMA without registering with DoT for trade license. The details are given in Appendix I.

This clearly indicates negligence of RMA in verifying supporting documents before issuance of AMC license and it also points out that these AMCs are operating illegally without having valid trade license. The comparison also revealed that there are only **three** standalone money changers holding both valid trade and AMC licenses.

ii. ***Money changer trade license issued by DoT but not registered with RMA for AMC license***

Notwithstanding the Foreign Exchange Rules and Regulations 2018 that requires any person other than authorized to apply for license from RMA to carry out money changing business, the RAA found that eight standalone Money Changers, out of 16, do not have Authorized Money Changers license from RMA (Appendix II). It was noted that these Money Changers have valid trade license but only two license holders have license to do money exchange business and the rest licenses are for retail, travel agent, and hotel businesses. Without having license for AMCs, these Money Changers are unauthorized to deal with any foreign exchange with any other person.

The RMA responded that they are currently verifying the validity of the trade license of all AMCs issued by Department of Trade (DoT). Further, the RMA stated that they are also in discussion with Department of Small and Cottage Industry (DSCI) regarding the authority for issuance of AMC license. Additionally, the RMA has issued a notification to individuals facilitating exchange services without AMC license to register with RMA.

As assured, the RMA should identify and address the discrepancies between DoT and intimate RAA through the Management Action Plan Report. Henceforth, the RMA should have clear arrangements with DoT as well as DSCI for further issuance of AMC licenses and intimate the same to RAA. There is also a need to strictly enforce the requirements of the Memorandum of Instructions (MoI) for Money Changers and raise awareness to all the AMCs on the need for a valid trade license.

iii. ***Hotels not issued with AMC license by RMA***

Similarly, the RAA carried out comparative analysis of list of hotels from TCB and the AMC licenses issued to hotels by RMA and noted that out 147 tourist hotels, only 30 hotels are issued with AMC licenses (as summarized in Table 2) indicating other 117 hotels might be dealing with foreign exchange without authorized license from RMA. The detailed information is given in Appendix III.

Table 2: Summary of tourist hotels issued with AMC license

Summary of Tourist Hotels Issued with AMC license	
Total Tourist Hotel as per Tourism Council of Bhutan	147
Total Hotels issued with AMC license	30
Hotels Without AMC License	117

The RMA clarified that it is not mandatory for all hotels to have AMC license. The RMA further explained that to curb illegal foreign currency exchange, tourists selling foreign currency to AMC's can reconvert the foreign currency after presenting the system generated cash receipt.

Furthermore, the RMA has also issued notification advising the general public facilitating exchange services to register with RMA for AMC license.

The RAA would like to stress there is a risk of doing unauthorised money changing business by not issuing AMC license to all the hotels. Therefore, the RAA emphasises on strong monitoring and urges the RMA issue AMC license to all tourist hotels to curb unauthorised foreign exchange transactions by the hotels.

3.2.2 Inadequate supervision over AMCs

The MoI issued by the RMA stipulates that the AMC license shall be issued only after the inspection of the feasibility of location and the existence of infrastructure.

However, the licenses were issued without inspecting the location and verifying whether infrastructure is in place or not. It was evident during the field visit to AMCs that except for Bhutan Money Exchanger and Bhutan Xchanger, there are no physical offices set up for exchange business by other standalone AMCs and yet, they are issued with AMC license.

Furthermore, amongst ten AMC agents visited by the RAA, only two agents have claimed to be visited by RMA more than two times since inception while three agents have stated to have been visited not even once. The rest claimed to have been visited once in more than three years.

Thus, it can be deduced that there is minimal supervision over AMCs which may result in not being able to effectively regulate foreign exchange transactions.

The RMA responded that 'The RMA has been conducting inspection of the AMCs on annual basis whereby they verify the infrastructure and transactions (reports available). The RMA prior to issuance of license conduct onsite inspection to verify infrastructure and location requirement. Further, we will also be initiating ad hoc inspection henceforth.'

The RAA agrees that RMA conducts annual inspection of AMCs but the current inspection is found to be inadequate as stated in the audit finding. Thus, the RMA should enforce strict monitoring and sporadic inspection for effective regulation of AMCs.

3.2.3 Comprehensive information on AMCs not captured in AMC System

It is important for RMA to assess the location of the AMC while issuing the license to ensure wider reach of such facilities. Thus, the AMCs' relevant information including the location should also be maintained in the AMC system. It is equally important to publish such information to general public and tourists in order to create awareness of such facilities in the market.

However, the RAA observed that neither the comprehensive information on AMCs are captured in the system nor are such information published on RMA's website for public awareness. Further, almost all the standalone money changers are clustered in the main town

of Thimphu; each located a few meters away from other. Some AMCs are even located in the vicinity of banking services.

As a result, the RMA does not have complete information on AMCs for monitoring purposes and people are not aware of AMCs thereby defeating the very objective of setting up such facilities.

The RMA, in their response, mentioned that 'We have the updated list of AMC which we continue to update upon renewal of AMCs. We are in the process of reviewing the AMC application form and will be incorporating changes with applicant details where necessary. And as recommended we will host the updated lists on the RMA website and AMC online system for monitoring purpose. Therefore we would appreciate if the above observation can be dropped.'

As stated earlier, the RAA verified the updated list provided and found that the list was same as the one given to the audit team before. The RAA reiterates that a comprehensive list of AMCs with their details should be captured in the AMC system for effective regulation.

3.3 Inadequacies in user access management

Secure user access management is crucial for safeguarding the information from unauthorized access and manipulation. User access control protects the confidentiality, integrity, and availability of assets (data files, application programs) from unauthorized modification, disclosure, loss, or impairment.

Having robust user access controls built in the information system would ensure users are provided with unique user credentials and access based on their roles and responsibilities. The RAA tested the adequacy of user access management within the IT Systems and observed the following lapses:

3.3.1 Improper procedures for user account creation

User accounts allow system users to access the IT systems to perform their day-to-day activities. As these accounts allow employees to access and use business-critical data, proper procedures should be in place for creating user accounts in order to mitigate risks associated with false user accounts.

The access control policy in the Information Security Policy of RMA specifies that the request for access to any IT System should come from HR and that appropriate access will be granted after verification and approval. Additionally, the ICBS operational procedural guidelines require that a user creation form should accompany the memo from the head of the Department.

The RAA also enquired on the current procedures and was made to understand that user accounts for RMA employees (using ICBS, INR & CC and AMC system) are created as and when a 'memo' is received from the HR. Further, for system users who are not employees of RMA, the user accounts are created based on 'memo' from the Department concerned. For

instance, the user accounts of AMCs using the AMC system are created based on a memo from the Department of Foreign Exchange and Reserve Management.

Yet, the aforementioned processes were found to be inadequate as evidenced by the documentation maintained for the same and the RAA noted the following procedural lapses:

i. User creation form did not accompany the memos from the Department concerned;
ii. There was no evidence of the verification and approval process in the Department of Information Technology (DIT);
iii. There was no documents regarding who created the user account;
iv. There was also no documentation on the access rights or profile or role (access matrix) assigned to the user account; and
v. At times user accounts were created upon verbal request to the DIT.

Such incidences imply that proper verification is not carried out and due process is not followed for user creation. This had happened because the Information Security Policy was not strongly enforced and also due to weak supervisory control. Weak documentations and improper procedures for user account creation could result in granting access to those who do not require access.

The RMA stated that the users are created based on the office memo, specifying rights and privileges, from the head of the department and the same memo is archived for future reference. In order to further streamline the procedures and controls, the department will reinstate template forms, adhering to the principle of least privilege, by the end of December 2019.

The RAA noted the response and the RMA should streamline user creation procedures and maintain proper documentation to avoid unauthorised users in the IT systems.

3.3.2 Shortcomings in user account management

Usernames and passwords are the most common authentication mechanism in a computer system. As such, usernames should be unique and consistent by following a particular naming convention to facilitate the IT administrators in efficiently managing the overall operations of the computer system and tracking user activities effectively. These naming conventions can be according to employee ID, CID or employee name. The RMA ICBS also follows a naming convention.

The RAA analysed the entire user IDs in the selected IT systems and found the following deficiencies:

i. Four generic or unidentifiable usernames such as ‘icbs’, ‘IAD’, were discovered as shown in table 3. These should not be permitted as a means of granting access to ICBS because generic ID makes it difficult to identify individuals and fix accountability if fraudulent activities are performed under these user accounts.

In this case, it would be even more difficult to attach accountability as the Employee ID given does not exist. Such generic usernames are provided access to all the screens of a module or an administration account. For instance, the user 'P' has been given access to all the screens of HRMS Module. Similarly, the user 'Icbs' has been granted the access for system administration.

Table 3: Generic usernames in ICBS

Username	Status of the user	Employee ID	Profile Name (Access given to the user)
Rsd	Active	37	Banking_RSD
Icbs	Active	67	Admin
P	Active	50029	ALL_HRMS
IAD	Active	50132	IAD_STAFF

ii. Likewise, the RAA found one generic user account in AMC system whose status is active with the user ID 'Test' and username 'RMA Test'. This might have been used for system testing and was not disabled since then.

iii. ICBS usernames are generated based on a particular naming convention. Seven usernames were found in ICBS that were not created based on the naming convention of the RMA as shown in Table 4. This defeats the purpose of having a consistent naming convention.

Table 4: List of usernames created without naming convention

Username	Status of the user	Employee ID	Profile Name (Access given to the user)
Tshering	Active	50038	Administrative_ Accounts
Tpem	Active	94	RMU_TPEM
Tdema	Active	34	BANKING_DIRECTOR
Dpelzom	Active	16	RMM
Damchu	Active	113	RMM CREATOR
PDema	Active	50049	PSD_VERIFIER
Kjurmey	Active	120	PSD_VERIFIER

iv. No naming convention exists for INR & CC and AMC system.

v. User accounts should be assigned to a particular role or profile which determines access rights and other details of the account. The users in ICBS are grouped and categorised into user profiles. However, the profiles are not logically created but actually created and assigned based on the user's name. For examples, the RAA found profile created solely for a user with profile names such as 'DCM_PELDEN', 'BANKING-KGYELTSHEN', 'DCM_DEKIYANGZOM', and many more of such cases.

vi. Users share their user credentials (username and password) with other users. This was observed amongst the INR & CC users and ICBS users indicating lack of security awareness amongst the users.

vii. The user credentials were saved in the web browsers for INR & CC and AMC systems as shown in Figure 6.

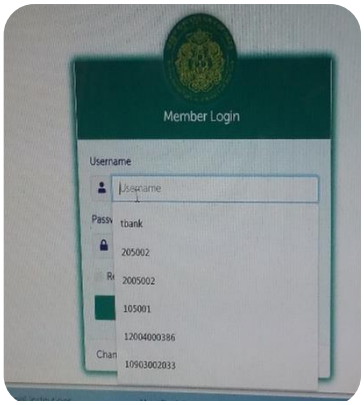


Figure 6: Saved usernames and password in INR & CC System.

Shortcomings in user account management indicate that due diligence is not followed to either maintain the naming conventions for usernames or disable temporary usernames once their functions are completed. Having generic usernames will make it difficult for the IT administrators to efficiently assign rights, track user activity and manage overall operations of the IT systems. This could also increase difficulty in fixing accountabilities in case of malicious activities performed in the systems.

Similarly, profiles are created for ease of system administration and to ensure that the user accounts are provided with the right access to perform his/her job responsibilities. Having profiles which are not logical and correct would ensue in granting users with inappropriate access in the IT systems.

The RMA explained that the username is created based on the internal naming convention. In few cases, there were shortcomings to adopt the same convention. Those usernames, which are not consistent, will be rectified accordingly.

As agreed, the RMA should ensure that proper user account management is maintained in order to minimize the risk of compromising integrity, confidentiality and availability of RMA data. Further, the RMA should ensure due diligence in user account management by following proper naming convention to avoid generic IDs in the IT systems, ensuring users do not share user credentials, and reviewing and reassigning user profiles periodically.

3.3.3 Weak password management

Password is one of the authentication methods used for restricting unauthorized access to information systems and data. Therefore, it is imperative to have an effective password management defining the "process of defining, implementing, and maintaining password policies".

The access control policy in the Information Security Policy of RMA stipulate all necessary requirements for password management; password must be

- masked when entered and stored in encrypted format,
- changed on first login,
- minimum length of eight characters,
- unique,
- alphanumeric (a combination of alphabet letters, numbers, and symbols) – also known as password complexity,
- and changed every 45 days (password aging).

Additionally, the policy also requires that password history be set at five numbers of last passwords. In other words, the history of last five passwords should be recorded in the system to avoid using the same password by the user.

The assessment of password controls revealed that the passwords are masked when entered as shown in Figure 7 and are stored in encrypted format.

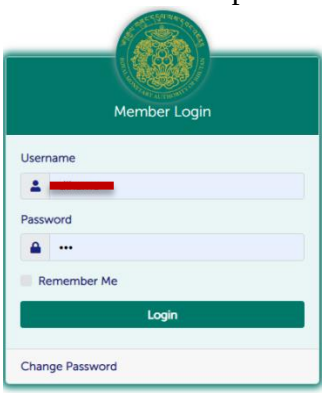


Figure 7: Password are masked when entered

However, the RAA observed the following lapses despite having an information security policy.

i. The system users are using passwords which are easy to guess. Password such as 123, rma@123, 567 etc. are used by system users in various instances. This indicates that the systems do not impose password complexity.

ii. The selected IT systems do not enforce the requirement of minimum length of password.

iii. The systems do not enforce password aging. In other words, there is no expiry dates for passwords or changing of passwords after a certain period which resulted in some of the system users keeping the same password since its creation.

iv. As apparent, the systems do not enforce the users to change their password on first login to change the default password created by the IT administrator.

These lapses indicate the non-enforcement of information security policy. Although an IT security policy which includes a password management was developed with the objective of securing the information assets and sensitive data from unauthorized access, modification and misuse, it is not well enforced and implemented within RMA. Additionally, it can be deduced that the security awareness of the users were found lacking even though the users were given security awareness trainings by IT personnel.

With such lapses, passwords could be easily deduced or cracked by potential attackers using techniques such as brute force attacks, etc., to gain access, and manipulate the systems and the data contained in them. It is important to note that the policy alone cannot ensure the security of the information system when the policy itself is not effective.

The RMA explained that the passwords are currently masked and stored in unreadable format. The RMA further commented that in order to secure the system, a strong password validation will be enforced to the users hereafter.

The RAA noted the plan to enforce strong password validation which will be verified in the follow-up audit. Moreover, the RMA should implement its information security policy to secure its information assets. There is also a need to sensitise the users on password controls.

3.3.4 Access rights not updated with change in role and responsibility

The system administrator should remove the access rights of a user upon change in role and responsibility, resignation or termination of an employee. This is to safeguard the system information from unauthorized access and misuse.

Upon review, the RAA noted that, the access rights given to the officials are not updated upon their transfer. While reviewing the ICBS system, the RAA noted four such cases even though these officials have been transferred to another Department with new role and the previous access right is no longer needed. The details are given in Table 5.

Table 5: Employee responsibility and their access rights to the system do not match

SI. No	Employee ID	Role Assigned in System	Designation	Department	User account status Active in the system
1	2013007	ALL_HRMS	Foreign Exchange Officer	Foreign Exchange and Reserve Management	Yes
2	2013013	PSD_VERIFIER	HR and Personnel Officer	Administration and Finance	Yes
3	2013038	RMM	Payment Systems Officer	Payment and Settlement System	Yes
4	2013012	PSD_VERIFIER	Internal Audit Officer	Internal Audit	Yes

As can be seen in table 5, the access right as a verifier in ICBS is not updated for one official who was transferred to Department of Internal Audit from Department of Payment and Settlement System. Similarly, three other officials are given access which is not in line with their responsibilities.

On a different note, one official who was working in Department of Foreign Exchange and Reserve Management have been transferred to Department of Macro Economic Research & Statistics but his previous access right was still active and used by one of the officials of Department of Foreign Exchange and Reserve Management.

The aforementioned lapses suggest that user access to ICBS are not reviewed and updated periodically. Assigning rights without considering users' responsibilities could lead to intentional or unintentional errors and opening rooms for fraud and malpractices.

The RMA responded that access rights and permission are created based on the request from the department. In few cases, such as during internal staff transfer, the rights and permissions have not been updated accordingly. The department will institute a process wherein any profile change/transfer will be informed to DIT to make concomitant changes in the system. However, the access rights have been updated in the online system. Considering the ratification, we request that the observation be dropped.

The RAA verified and found that the user access rights have indeed been updated. Further, the RAA noted that proper procedures will be established between the HR and DIT to update the user access as soon as an official is transferred or separated which will ensure strong access control mechanism.

3.4 Weaknesses in application security

Application security is the process of developing and implementing security features within the IT systems to prevent security vulnerabilities against threats such as unauthorized access and modification. These threats to IT systems can be internal and external. In the case of ICBS, it is predominantly internal threats since ICBS is used inside the RMA. On the other hand, the INR & CC and AMC systems being web-based should be protected against external threats such as cyber-attacks.

Cybercrimes are increasing at a rapid pace and cybercriminals are constantly attacking the critical infrastructures and networks in order to discover any inherent vulnerability; which can be exploited to steal sensitive and valuable financial and business information.

The RAA assessed the vulnerabilities in the selected IT systems and observed the following deficiencies.

3.4.1 Session timeout not set for the system

Session timeout is an important security feature that needs to be incorporated in an IT system. It determines how long a device may remain active before it logs off. After which, a user must perform authentication again to start using the system.

The system should automatically log out after certain period of inactivity. This security feature prevents invalid and unauthorized personnel from accessing the systems when the authorized person is away from their workplace and has forgotten to log out of the system.

While verifying the systems, the RAA noted that the ICBS, INR & CC and AMC have not set session timeouts for their systems. As a result, the systems remained active for unlimited period of time unless logged out manually. In Figure 8, the AMC system remained active even when it was idle for more than two hours i.e., from 12.23 PM to 2:57 PM. Similar controls were also found lacking in both ICBS and INR & CC systems as well.

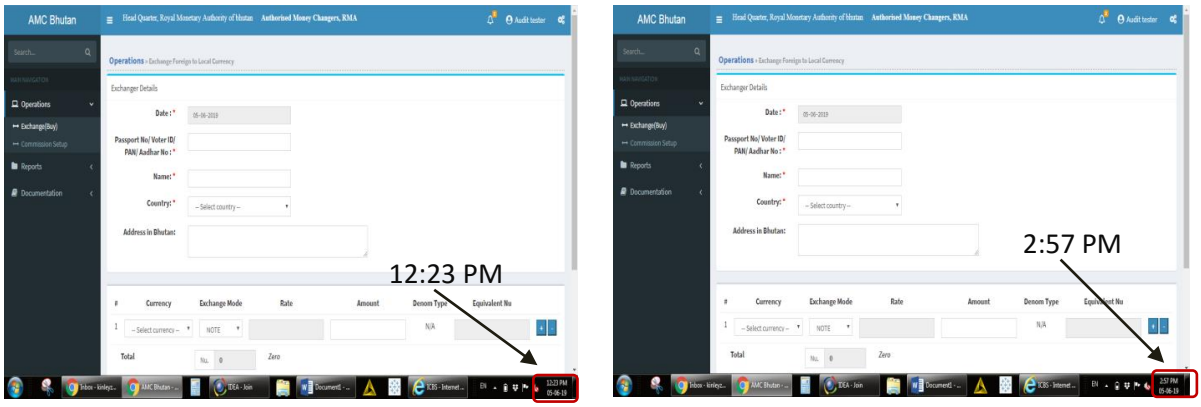


Figure 8: Session remaining active in AMC system even after lapse of more than two hours

Not setting session timeout will allow unauthorized attackers (usually working in the same organization) to access the other employee's system and manipulate the information and data.

This will also subsequently hinder the process of assigning accountability for the actions as the real culprit cannot be traced from the account activity.

The RMA argued that session timeout is currently configured at the desktop level, which will automatically log out the users within a predefined idle time. The RMA assured that session timeout will be developed and calibrated for each system as per recommendation.

The RAA would like to clarify that if session timeout is configured at desktop level then the users will be logged out along with the IT system. However, as stated in the audit finding, the RAA test-checked and found that there is no session timeout for the IT systems as well as at the desktop level. As assured, the RMA should develop session timeout for each of the IT systems.

3.4.2 Unlimited unsuccessful logon attempts

The number of unsuccessful logon attempts should be limited so that unauthorised users do not gain access to the IT systems. The System Administrator should limit the number of failed logon attempts so as to prevent the attackers from repeatedly trying various combinations of usernames and passwords to gain access to the information system; this attack technique is known as Brute Force Attack. The Information Security Policy of RMA stipulates to allow only three number of unsuccessful logon attempts.

Nevertheless, the RAA noted that the systems in the RMA (ICBS, INR & CC and AMC) allows unlimited logon attempts (be it invalid usernames and passwords) as shown in Figure 9.

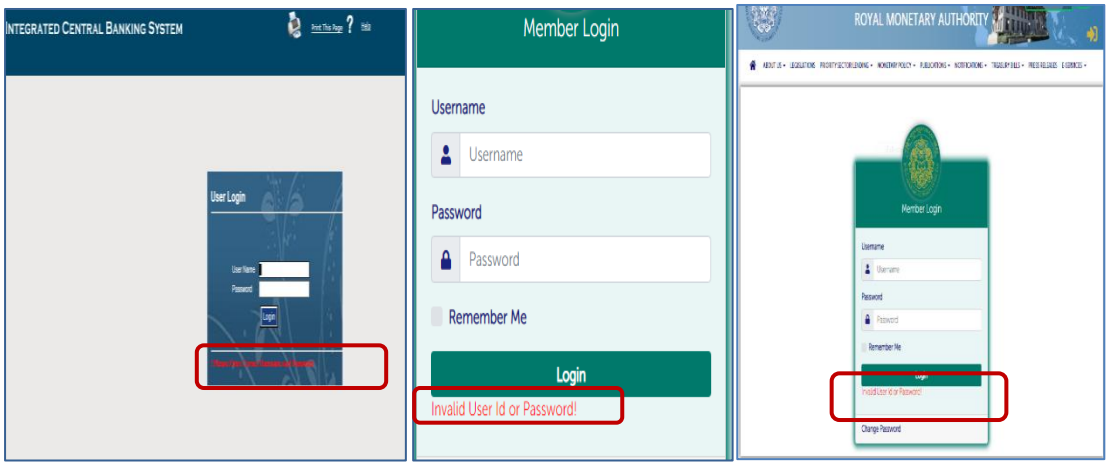


Figure 9: IT systems allowing unlimited logon Attempts with invalid password and user name

As a result, it leaves the IT systems vulnerable to brute force attacks, which inherently leads to unauthorized access. This could result in serious consequences such as information misuse and losing control of the information systems.

The RMA assured that number of unsuccessful logons will be limited to 3 attempts and after that the user will be disabled. It was initially kept open to provide flexibility to diverse users.

The RAA noted the reason for keeping it open initially and the assurance given which will be verified during follow-up.

3.4.3 Inadequate input control

Input controls are automated computer controls designed to ensure that data entered by users are valid, complete, and sensible. Input controls should be implemented in IT system so that incomplete, duplicate, invalid and erroneous data are rejected at time of data entry. Likewise, the IT systems implemented in RMA should also have robust input controls to ensure data completeness and reliability.

Upon the review of input controls in the ICBS, AMC, INR & CC systems, the RAA noted good input controls implemented in ICBS whereas other two systems have weak input controls resulting in following lapses:

3.4.3 Acceptance of invalid data by AMC and INR & CC systems

3.4.3.1 Invalid Names and Contact Number

Individual details such as names, CID, contact number, and income sources are entered into INR & CC system while availing INR. As such, in order to prevent the double issuance of INR to the same individual within the allowable quota time of one month, valid names and other correct details must entered into the system. Nonetheless, the RAA found invalid names of individuals in the INR & CC system. The system has accepted numbers as names, which otherwise should be in letters format. In addition, the system does not perform format checks for contact numbers thereby allowing invalid range of contact number (more than or less than eight digits) as shown in Figure 10.

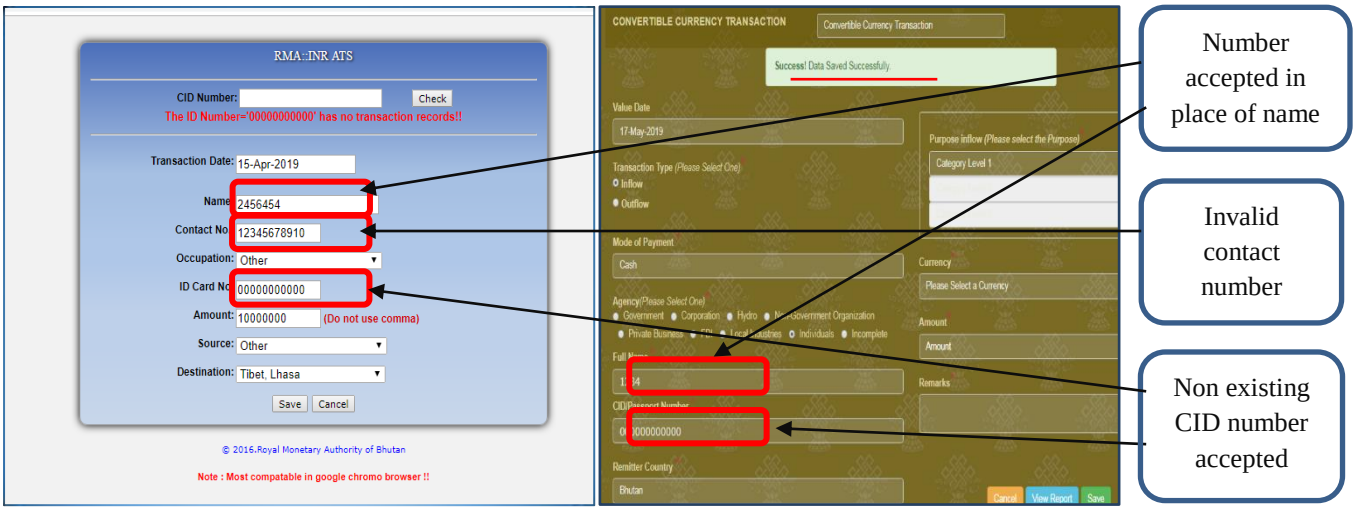
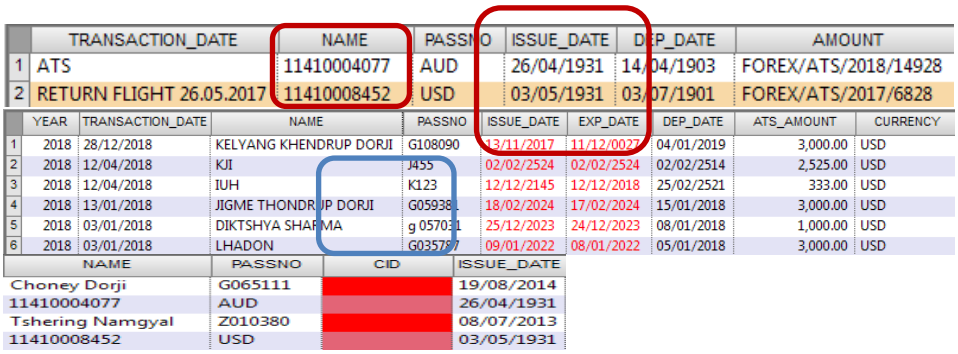


Figure 10: INR & CC system accepting invalid names, CID No. and Contact Numbers of individual

Similarly, in case of issuance of USD ATS, the system also accepted invalid or empty inputs. While analysing the data for 2018, the RAA noted several instances where invalid inputs such as the name of person entered in numeric format, the passport expiry date being same or later than the issue date, and blank CID numbers as depicted in Figure 11.



	TRANSACTION_DATE	NAME	PASSNO	ISSUE_DATE	DEP_DATE	AMOUNT
1	ATS	11410004077	AUD	26/04/1931	14/04/1903	FOREX/ATS/2018/14928
2	RETURN FLIGHT 26.05.2017	11410008452	USD	03/05/1931	03/07/1901	FOREX/ATS/2017/6828

	YEAR	TRANSACTION_DATE	NAME	PASSNO	ISSUE_DATE	EXP_DATE	DEP_DATE	ATS_AMOUNT	CURRENCY
1	2018	28/12/2018	KELYANG KHENDRUP DORJI	G108090	13/11/2017	11/12/0027	04/01/2019	3,000.00	USD
2	2018	12/04/2018	KJI	J455	02/02/2524	02/02/2524	02/02/2514	2,525.00	USD
3	2018	12/04/2018	IUH	K123	12/12/2145	12/12/2018	25/02/2521	333.00	USD
4	2018	13/01/2018	JIGME THONDRUP DORJI	G059381	18/02/2024	17/02/2024	15/01/2018	3,000.00	USD
5	2018	03/01/2018	DIKTSHYA SHARMA	g 057031	25/12/2023	24/12/2023	08/01/2018	1,000.00	USD
6	2018	03/01/2018	LHADON	G035787	09/01/2022	08/01/2022	05/01/2018	3,000.00	USD

NAME	PASSNO	CID	ISSUE_DATE
Choney Dorji	G065111		19/08/2014
11410004077	AUD		26/04/1931
Tshering Namgyal	Z010380		08/07/2013
11410008452	USD		03/05/1931

Figure 11: Lack of input controls while issuing USD ATS

The RMA explained that names field will be developed to accept only alphabets and the contact numbers to accept only numeric digits by December 2019.

The RAA noted the same which will be verified during the follow-up audit.

3.4.3.2 Invalid CID number

CID number is used an identifier to check the frequency of INR issued to individuals as well as the limit of ATS (other currencies) in the INR & CC system. Thus, it is important to capture valid CID numbers in the system, which should be of 11 digit number. However, while analysing the data of 2018, the RAA noted 172 cases where CID numbers consisting of less than 11 digits were accepted by the system.

The system does not check the validity of CID numbers entered and even allows random numbers in place of CID numbers as depicted in Figure 12. Further, the system does not automatically populate relevant fields while entering the CID number, instead, the system users need to enter these details manually which could lead to entering incorrect data or invalid data.

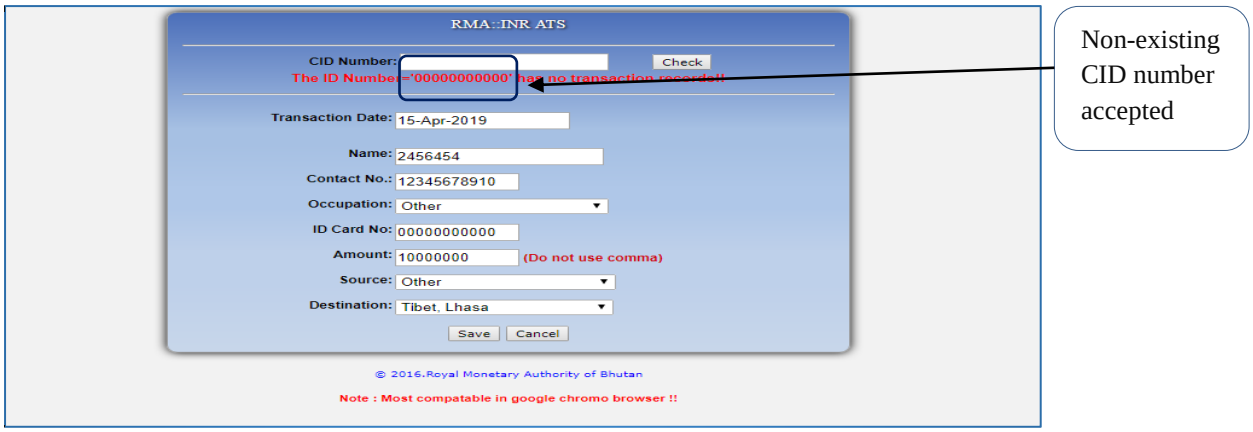


Figure 12: Random CID number accepted by INR and CC system

Weak input controls in the system have led to acceptance of invalid data in INR & CC System, which in turn does not control the issuance of INR based on correct CID numbers and individual details forgoing the very objective of limiting the INR within the quota time of one month using CID as unique key identifier. Not incorporating robust input controls in the system would result in generating inaccurate and unreliable reports that will impede in making informed and correct decisions.

The RMA clarified that the current system design accepts CID less than 11 digits since there are cases wherein they have to release INR to different card holders, such as special resident permits having different CID length. Nevertheless, the RMA will incorporate a new field for special permit number and CID field will be restricted to accept 11 digits.

While noting the changes to be implemented, the RMA should also be vigilant and make changes to other data fields as and when such weaknesses are discovered. In the future, the RMA should implement strong input validation in all of its IT systems.

3.5 Lack of validation controls in INR & CC

Validation controls ensure data correctness and accuracy. Thus, validation checks or controls must be implemented in the IT Systems to identify and reject incorrect and inaccurate data.

With the INR & CC not only can the INR and CC inflow and outflow be traced but the validation of the customer requisition for foreign currency (CC or INR) using Citizenship Identity (CID) can also be performed. For instance, the system will alert and decline the requisition if the particular CID has already availed the annual quota of USD 3000. This validation is instituted to ensure that the foreign exchange transactions for various purposes are within the limits established by the RMA in Foreign Exchange Rules and Regulations 2018 and Foreign Exchange Operational Guidelines 2018.

Upon review of validation controls in the selected IT systems of RMA, the RAA noted weak validations in INR & CC system, which subsequently resulted in the following deficiencies:

3.5.1 INR issued more than allowable limit

As per Foreign Exchange Operational Guidelines 2018 and Notifications issued by RMA, under the Annual Travel Scheme, an individual is eligible for 10,000 INR monthly from March to September and 30,000 INR from October to February. Accordingly, validation control must be embedded in the INR System to reject when the INR issued amount is more than the maximum allowable limit. However, the analysis of 2018 data showed 55 cases where the INR issued was more than allowable quota of 10,000 as provided in Appendix IV and 55 cases where INR issued amount exceeded 30,000 as exhibited in Appendix V. It was noted that these instances were a result of not having robust validation control in the system.

Furthermore, the RAA conducted deeper analysis and observed instances showing same individuals availing multiple times of ATS on the same day exceeding the limit ATS amount.

In an instance, INR was issued eight times to a single person on the same day amounting to 160,000 INR. Similarly, there were other instances where INR was issued three to two times to individuals on a single day.

The RAA also found several instances where INR was issued to same persons from different regional offices within a month wherein the total amount exceeded the maximum limit. In 2018 alone, there were six instances where three individuals has availed INR from Thimphu as well as from Phuentsholing in the same month as shown in Figure 13.

	TRAN_DATE	MONTH	CID	OCCUP	AMOUT	SOURCE	DEST	OFFICE
1	06-12-18	12	11603002424	Other	30,000.00	Savings	India, Delhi	RMA, Thimphu
2	10-12-18	12	11603002424	Corporate Employee	20,000.00	Savings	India, Kolkata	RMA, Phuntsholing
3	22-10-18	10	11704000277	Business owner	30,000.00	Savings	India, Sikkim	RMA, Phuntsholing
4	08-10-18	10	11704000277	Civil Servant	30,000.00	Salary	India, Amarnath	RMA, Thimphu
5	28-06-18	6	11915000257	Civil Servant	10,000.00	Salary	India, Siliguri	RMA, Phuntsholing
6	07-06-18	6	11915000257	Business owner	5,000.00	Savings	Nepal, Lumbini	RMA, Thimphu

Figure 13: Double issuance of INR to same person from different offices within the same month

The RMA stated that they will enforce strict validation in the system to check the limit for INR without exception to the rule. Further, they will train the end users on how to check the limits and input the requisition. In some cases, the reasons could be attributed to the Internet connectivity issues wherein the users tend to save same record multiple times by clicking on save button.

As the RMA is already made aware of the results of having a weak save validation, the RMA, as assured, should enforce validation checks to ensure that the INR issued does not exceed the quota depending on the purpose.

Additionally, the RMA should implement duplicate checks in the save button validation so that even with internet connectivity issues, duplicate data is not saved in the IT systems.

3.5.2 USD ATS exceeded the quota

As per annexure I of Foreign Exchange Operational Guidelines 2018, the Annual Travel Scheme (ATS) USD quota for an individual is USD 3000.

Upon analysis of data, the RAA noted cases where the USD ATS amount issued to individuals exceeded the maximum limit specified in the Foreign Exchange Operational Guidelines 2018. A summary of the instances is portrayed in Table 6 and the details of the same are given in Appendix VI.

Table 6: Issuance of USD ATS exceeding the USD 3000 quota in one year

CID No	No of times issued in 2018	USD ATS Amount
10806002196	7	21000.00
11410003171	4	6000.00
EC0301415	3	4350.00
11806000433	3	3600.00
11410005063	3	6000.00

CID No	No of times issued in 2018	USD ATS Amount
11211001701	3	9000.00
11704003901	2	3403.00
11513004660	2	3084.00
11513004068	2	4620.00
11512003546	2	4610.00
11410004061	2	5000.00
11410001570	2	6000.00
11312003470	2	3292.00
10802000481	2	6000.00
10605004460	2	6000.00
10211002974	2	4307.00

The analysis revealed that an individual has been issued USD seven times aggregating to USD 21000 on the same day implying that the same record must have been saved seven times. While for other cases, the USD ATS must have been issued beyond allowable quota in the same year.

The RMA assured to enforce strict validation control to check the quota limit. However, in some cases, the reasons could be attributed to the Internet connectivity issues wherein the users tend to save same record multiple times by clicking on save button.

As responded, the RMA should enforce strong validation controls to ensure compliance to Foreign Exchange Operational Guidelines 2018. As stated earlier, the RMA should also implement duplicate checks in the save validation to avoid duplicate records in the IT systems.

3.5.3 INR system accepting amount below the minimum amount

Likewise, while reviewing the INR data of 2018, cases were also found where INR amount issued was less the minimum amount allowed as per the Foreign exchange operational guidelines 2018. As per the guideline, the minimum INR amount to be issued should be ₹500 per incident. However, instances in the system showed INR of amount 0, 100, 300 issued to individuals as showed in the Figure 14 below.

	TRAN_DATE	NAME	OCCUP	CID	AMOUT	DEST	OFFICE
1	25-10-18		Other	20244889911	0.00	India, Bodhgaya	RMA, Thimphu
2	06-09-18		Business owner	10906002169	100.00	India, Sikkim	RMA, Thimphu
3	28-11-18		Other	10203002582	300.00	India, Sikkim	RMA, Thimphu
4	10-12-18		House Wife	11514004354	300.00	India, Sikkim	RMA, Mongar

Figure 14: Issue of INR below the minimum specified in the guideline

It is quite surprising that even zero amount was recorded and accepted in the system. All the above lapses primarily occurred due to lack of validation controls instituted in the INR & CC

System. Absence of such checks in the system would defeat the purpose and intention of the system for which it was built i.e. to effectively control and monitor the inflow and outflow of the convertible currency. This could also lead to improper control of INR outflow as INR can be issued multiple times to the same individual with different random numbers as CID.

The RMA argued that as per Foreign Exchange Operational Guidelines 2018, Annex II, the total ATS per month is 10,000 and there are no provisions stating minimum INR amount to be issued should be INR 500. Therefore, this observation can be dropped.

While accepting the response and the fact that the Foreign Exchange Operational Guidelines 2018 is silent on the minimum INR amount to be issued, the RAA would like to assert the RMA should specify the minimum INR amount as it is quite surprising that the system even accepts zero amount. The RAA noted instances of INR300 being issued which is quite unrealistic. Therefore, the RMA should implement strong validation controls in its IT systems.

3.5.4 INR & CC system contains list of countries where INR is not required

According to Foreign Exchange Rules and Regulation 2018, INR is only issued if the country of destination is India or Nepal. In other words, for any INR transactions, the list of destination should contain India and Nepal.

In contrary, upon verification of the system, the RAA noted that the INR & CC system listed other country destinations such as Sri Lanka and Tibet where INR is not required as given in Figure 15.

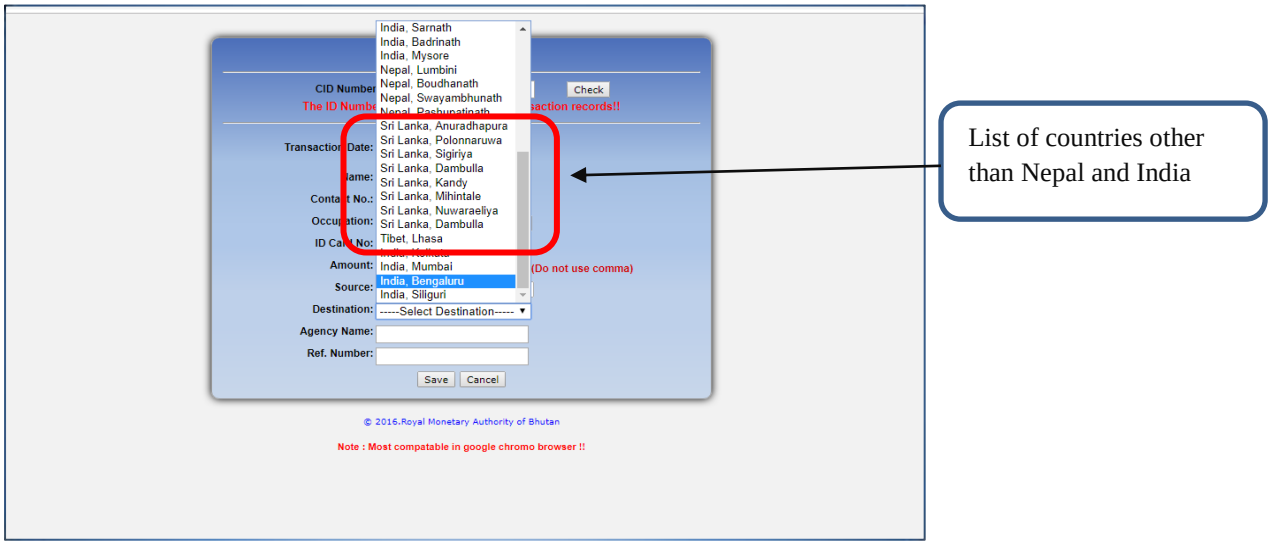


Figure 15: Country of destination other than India and Nepal

Since there are destinations other than India and Nepal in system, INR can be issued for those destination which should have been prohibited. While reviewing the INR data of 2018, the RAA found eight instances where INR was issued for Tibet as country of destination and

three instances for Sri Lanka as country of destination indicating non-compliances to Foreign Exchange Rules and Regulation 2018.

The RMA clarified that destinations such as Sri Lanka and Tibet were listed in the system because the final destinations of the travel is considered. The INR is issued for such destinations if the travel is routed via India for on-route expenses. Considering the above response, the RMA requested that the observation be dropped.

The RAA acknowledges the response. Nevertheless, the on-route destination should be captured in the system while destinations such as Sri Lanka and Tibet could be captured as the final destination in the system. This would ensure that accurate information is recorded and generated by the INR & CC system as the INR being issued for destinations such as Sri Lanka and Tibet would be incorrect. In this way, the management can also be made aware when the report for INR outflow is presented to them.

3.6 Improper segregation of incompatible duties in ICBS

Segregation of Duties is a control that facilitate separation of work responsibilities such that one person does not have access to or control over all critical stages of information handling process. Segregation of duties could be enforced through manual and/or automated measures in the form of access privileges in IT systems.

In this context, the RAA test checked the automated segregation of duties by reviewing the access privileges for ICBS users and ascertained if the system prevents the same user from performing all the critical functions in system.

Upon verification, the RAA noted that the ICBS has three-layer controls; creator for preparing the transaction, verifier to verify the transaction and authorizer to approve the transaction. The creator cannot verify and authorize and same applies to verifier and the authorizer as well.

While the RAA noted the implementation, the system does not enforce this control and as a result the ICBS allowed some users to perform all three roles irrespective of their designation and role as shown in Figure 16.

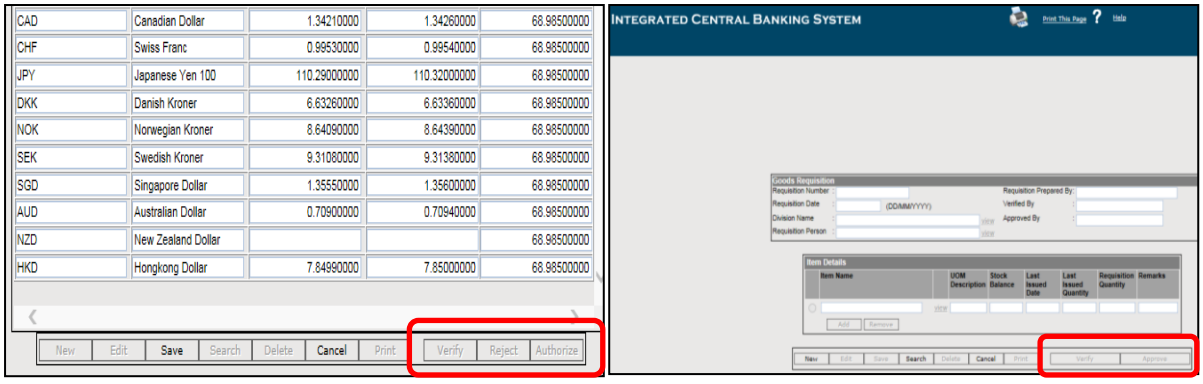


Figure 16: Active verification and authorization option for creator

The RAA found that the same official can create a transaction and also verify the same transaction. In some cases, the same official can also approve or authorise the same

transaction. For instance, the person preparing vouchers in ICBS can also verify and approve the vouchers. In particular, the following were observed from the ICBS data analysis for 2018 as summarised in Table 7.

Table 7: Instances of transactions created and verified and in some cases, approved by the same official

Area of operation	Instances of transactions created and verified by same official	Instances of transactions created, verified and approved by same official
Currency management and currency chest operations	745	606
Foreign exchange rate	173	172
Voucher preparation in banking and administrative accounting	770	429

Table 7 confirms the existence of improper segregation of incompatible duties in ICBS. The officials claim that the access rights for all level of controls were given to an individual so that one can replace and take up the job of another when that official goes on leave.

The aforementioned inadequacies in segregation of duties happened primarily due to inappropriate granting of access privileges to ICBS users. In other words, some users were granted rights more than what they are required to perform their roles for convenience sake. While it is understandable at times that it is not practical and cost-effective to segregate duties, compensating controls such as periodic monitoring should be implemented by the management.

Absence of effective segregation of duties could add the risk of (1) more opportunities of misconduct, (2) deliberate or unintentional malpractice or errors, and (3) errors and fraud will not be detected and addressed in a timely manner.

The RMA explained that the ICBS design is based on maker-checker concept, consisting of creator, verifier and authorizer. The RMA further commented that while it is the responsibility of the department concerned to segregate functional duties, the Department of Information Technology will make concerted effort to enforce maker-checker principle.

While noting the response, the RAA would like to emphasise that the responsibility lies with the RMA as a whole to implement segregation of duties and there is a need to properly segregate incompatible duties. Further, it is understandable that there could be manpower shortage and hence, not practical and cost-effective to segregate duties, and yet, compensating controls should be implemented by the management.

3.7 Lack of adequate surveillance in the systems

Surveillance of business-critical data in ICBS, INR & CC and AMC can be carried out through audit trails and logs. Audit logs and trails can provide a means to help accomplish several security objectives, including individual accountability (trace user activities), reconstruction of events (actions performed on the RMA systems), fraudulent activities or inadvertent changes, and identification of system errors. Therefore, audit trails and logs form

an essential component which should exist in the IT systems to enforce accountability and should be periodically analysed to detect any control weaknesses in the system.

During the process of audit, it was found that the IT systems have minimal logging capability; user logs. The user logs record information on user activities such as who entered the data with date and time stamps. Additionally, the ICBS maintains user logs not only for data entry but also for data verification and authorisation along with edited details if any in the database corresponding to each transaction.

Although these audit logs are maintained, the following inadequacies were observed.

i. The design of the audit logs in ICBS is such that it accepts blank data. In other words, transactions can be approved without recording the details of the user as shown in Figure 17. With these exceptions, one cannot trace the transaction back to the user. This means that if there are any fraudulent activities in these transactions, it cannot be established who had performed that activity.

CREATEDBY	MODIFIEDBY	VERIFIEDBY	AUTHORISEDBY
66		85	
50005		50071	
85		86	
86		79	
86		79	

Figure 17: ICBS accepting blanks in Authorised column

ii. There is no log maintained for deleted vouchers to keep a record of deleted vouchers with details such as deleted voucher number, who deleted it along with date and timestamp. Instead, the record for any deleted voucher is maintained physically.

iii. The audit logs and trails never monitored or reviewed to gain insights into the system activities since its inception.

Lack of adequate audit trials and logs in the system could potentially result in addition or modification of transactions by unknown user. As a result, system administrators might be unable to enforce accountability when there is a misuse of system and its data.

Without a review of audit trail data, malicious activities, system errors, fraudulent activities and intrusions could go undetected which could consequently disrupt the IT systems from functioning.

The RMA responded that currently, the system logs transaction details, timestamp and user IDs. Based on the recommendation, the logs will be further reviewed to capture end-to-end trails and the logs will be timely monitoring of the logs.

As assured, the RMA should develop and maintain adequate and appropriate audit logs and trails in IT systems, and establish a review mechanism for audit logs that not only serves as a detective measure and post incident management but also as a preventive measure to avoid security breaches in the first place.

3.8 User training not provided

Successful IT implementation depends on the competence of the system users. In order to improve the effectiveness of the system through reduced errors and increased productivity, it is essential to provide training to all users including the IT technical team. When the users are competent on the system, the services will be delivered without any hindrance.

Additionally, knowledge transfer has also been recognized as one of the key success factors for the implementation for any IT system. When the outgoing officials leave the department, there should be a process of knowledge transfer on the system know-how and the relevant process workflows between incoming official and outgoing official to ensure smooth and continuity of the responsibilities.

Upon review, the RAA noted the following with regard to user training and knowledge transfer.

i. Only minimal guidance is provided for navigating the IT system by senior officials to new recruits or to those who are newly transferred;
ii. Formal user trainings were never conducted since inception of the IT systems. According to the response received from the interview questions distributed among the system users, it appeared that the system users are neither involved in the development of the system nor given any formal trainings;
iii. There were no procedures in place to ensure that the business process workflows and system know-how are handed over by the outgoing officials to incoming officials which implies that there is no proper knowledge transfer mechanism when there is a change in officials handling the system.

Due to lack of proper training and familiarization on the system and due to lack of knowledge transfer between outgoing and incoming officials, most of the users are still not fully competent with the systems and still not aware of the flow of their work. This was also evident from the case presented below.

Case of system users not fully aware of business process

The system users in Department of Foreign Exchange and Reserve Management are not aware of the formulae and procedure for deriving exchange rate of the foreign currency and calculating the bullion rates. Due to this, the computed exchange rate in the ICBS is manually compared with the rates computed in MS Excel for correctness.

In order to explain the complete process flow and the formulae inserted in system, the officials have to refer to those officials who were previously with the department.

Although the use of system can be learned by the system users even without getting formal training as the job is repeated in nature, it is imperative that one should know the real process and nature of their job which is done through system. If the system users are not given proper training on the system, and if the trend of training successive officials is followed in same manner, the officials will not know the process flow of their own department.

The RMA responded that the end users will be trained on how to check the limits and input the requisition for INR & CC system. Additionally, they will also provide user training for all other system.

While acknowledging the response, the RAA also urges the RMA to train users not only on the IT systems but also on the workflow of business processes for smooth functioning of the business. The RMA should ensure that there is a process for transfer of knowledge in the organisation.

3.9 Lack of Business Continuity Plan

It is vital for every organization to prepare and plan for business continuity in an event of disaster or disruption to their business as it ensures normal operation of business in the event of interruption with minimal impact. Disruption to the critical systems data due to unexpected incident might not only cause financial loss but also could affect the credibility of the organization. Hence, it is crucial to develop Business Continuity Plan (BCP) to support the business organizations in ensuring continuity of their business operation during and after a disaster.

Although the RAA noted existence of disaster recovery plan, the RMA still lacks comprehensive business continuity plan detailing all strategies that RMA will undertake during emergencies and interruptions to its business operations ensuring continuity of RMA services to the end users. The business continuity plan should consists of:

1. Business impact assessment;
2. Responsible persons in case of emergencies along with contact information;
3. Analysis of organizational threats;
4. A list of the primary tasks required to maintain the continuity of organization business operations;
5. Assessment of critical assets including information and data;
6. Information on data backups and organization site backup
7. Collaboration among all facets of the organization

Since disaster recovery plan primarily includes only getting systems up and running after an incident, not having comprehensive BCP could thwart the management in implementing effective measures to ensure continuity of normal business operations in the event of disaster with less impact.

The RMA stated that database backup is performed daily at the primary site and stored at the primary and Phuentsholing backup site.

The RAA acknowledges the initiative of the RMA in having a DR site. Nonetheless, the RAA stresses that business continuity is not only about taking database backup but contains all critical functions or activities that need to be performed for ensuring continuity of business operations. Thus, the RMA should develop comprehensive Business Continuity Plan.

3.10 Inadequate system documentation

ICBS, INR & CC and AMC support critical functions of RMA and as such, comprehensive and up-to-date documents related to system have to be readily available. Adequate documentation has to be available to aid ICT officials during maintenance and enhancement activities, to acquaint users with the function and proper use of the IT systems, and to facilitate auditing of the IT systems. System documents would also enable RMA to manage changes and track progresses and enhancements made thus far.

In this regard, the RAA ascertained the existence and adequacy of documents to support future enhancement and maintenance and found it to be inadequate. There is no adequate documentation for the whole system development process (ICBS, INR & CC and AMC) in RMA except for service requirement specifications (SRS) of ICBS.

Currently, the IT officials have to manually go through all the tables particularly in ICBS as and when there are enhancements or maintenance for the system. This is extremely time intensive and solely based on the IT personnel's experiences and tacit knowledge. However, such knowledge will be lost if the knowledgeable person leaves RMA as there are no system are to capture such knowledge in documents for future enhancements and supports.

Since there is no proper documentation, it implies that the systems in the RMA were developed without following a proper set of procedures. Further, without adequate documentation, it is not clear if the stakeholders – both internal and external – were consulted to understand workflow processes and user scenarios and it can be also construed that there was no testing conducted to ascertain the reliability of the IT system and reports generated. Inadequate documents might lead to operational and maintenance difficulties.

The RMA explained that system documentation pertaining to ICBS, such as the software requirement specification, design document, minutes and memos are available for reference.

While noting the existence of some system documentation pertaining to ICBS, the RAA reiterates that adequate system documentation should be available for all IT systems for future reference and enhancements.

CHAPTER 4: RECOMMENDATIONS

Based on the issues pointed out under Part 2 in chapter 3, the RAA has provided recommendations aimed at enhancing efficiency and effectiveness of ICBS, INR & CC and AMC systems in RMA. The recommendations are as discussed below:

4.1. RMA should ensure that the IT systems developed are used for intended purpose

Recognizing the benefits and potential of IT in improving the efficiency of its operation, the RMA automated its business processes by developing relevant IT systems. As system development entails huge financial investment, it is imperative to ensure that the intended objectives of developing the system are met and the system is used optimally in order generate return on investment. However, the RAA noted that the IT systems selected for review are either not used optimally or do not cater the needs of the users. In other words, the IT systems do not adequately support RMA's business operations. Additionally, the INR & CC system, which was developed to monitor the convertible currency (CC) and Indian Rupee (INR) outflow and inflow of the country, does not generate comprehensive INR & CC outflow and inflow report.

As such, RMA should:

- insist AMCs to use the AMC system in order to ensure optimal utilization of the system which will also enhance regulation of AMCs; and
- ensure the use of INR & CC system by all the system users including banks and relevant RMA officials for all INR and CC transactions in order to generate comprehensive INR and CC reports. This will also help in monitoring near to real time INR and CC transactions.

4.2. RMA should institute robust IT controls in ICBS, INR & CC and AMC Systems

The RAA noted inadequate and weak IT controls in ICBS, INR & CC, and AMC Systems, which will lead to unauthorized access, security breaches, and generation of inaccurate and unreliable information. Thus, RMA should institute and enforce robust IT controls in the systems to maintain the integrity and reliability of the IT systems particularly in the following areas:

- ensure access control mechanism to assign access rights and privileges based on 'need to know' and 'least privilege' principles in order to mitigate the risk of unauthorised access, data modification, disclosure, or loss;
- enforce information security policy to ensure effective IT security management;

- implement strong input controls so that INR & CC system does not accept invalid, garbage, and duplicate data so as to avoid processing incorrect or illogical information;
- implement strong validation controls in INR & CC system so that the ATS (both INR and USD) are issued within the allowable limit or quota;
- institute proper user account management for creating user accounts, avoid creation of generic user accounts, follow proper naming convention;
- institute effective password management including enforcement of minimum password length, requirement of complex passwords (combination of alphanumeric & symbols), enforcement of password aging, change of password after first login, and prohibition of password sharing;
- address vulnerabilities found in application security in order to protect the IT systems from possible external threats;
- login attempts with invalid passwords or usernames and session timeouts should also be limited in order to reduce the risks of gaining unauthorized access;
- develop comprehensive Business Continuity Plan that can be implemented in the event of incident or disaster to ensure continuity of their normal business operation; and
- train the users so that they have adequate knowledge of business processes, workflows and security awareness.

4.3. RMA should institute mechanism to enhance regulation of Authorized Money Changers

RMA initiated Authorized Money Changers to monitor and regulate the exchange of foreign currencies and also to curb illegal money exchange practices. The RAA noted lapses in the management of AMCs and recommends the following:

- At present, the RMA lacks a comprehensive registry Authorized Money Changers (AMC). Considering the importance of registry of AMCs for effective monitoring and regulation of foreign exchange transactions, it is imperative that the RMA maintains accurate, comprehensive, reliable and up-to-date registry of AMC in the AMC system;
- Further, the RAA noted discrepancies between the list of AMC licenses issued by RMA and Department of Trade (DoT) resulting in carrying out money exchange businesses without having valid licence. Therefore, in order to curb illegal money exchange business, the RMA should take initiatives to verify and address those discrepancies noted and coordinate with DoT for issuance of AMC licenses in the future;

- RMA should enforce the requirements prescribed in Memorandum of Instructions (MoI) for Money Changers particularly production of valid trade license from DoT for carrying money exchange business; and
- conduct periodic inspection and monitoring of AMCs for effective regulation and for optimal utilization of the system.

4.4. RMA should enforce proper segregation of duties

It is important to separate responsibilities and roles amongst individuals particularly those in financial function so as to minimize the risk of occurrence of fraudulent activities and deliberate or unintentional malpractices/errors and this can be implemented both in manual and automated system by instituting proper segregation of duties. Although the segregation of duties is implemented in the ICBS system in the form of maker-checker, the RAA noted that this concept is not fully enforced in ICBS System.

Thus, RMA should ensure that maker and checker concept is enforced to implement proper segregation of duties according to the roles and responsibilities.

CHAPTER 5: CONCLUSION

Recognising the role and mandate of RMA to ensure monetary stability in the country and the significance of IT systems to achieve this mandate and enhancing its operational efficiency, the RAA has carried out the IT audit of ICBS, INR & CC, and AMC covering the period 01 January 2018 to 31 December 2018. The audit was focussed primarily on whether the selected IT systems made the internal operations and regulation of foreign currencies efficient and effective. In addition to this, the audit also assessed the adequacy of general and application controls in the IT systems under review.

The implementation of ICBS has automated the functions of RMA and resulted in capturing essential information of RMA's operations. Similarly, the INR & CC system has made it easier to monitor the limits on foreign currencies for Annual Travel Scheme, and the AMC system has facilitated the exchange of foreign currencies through AMC agents.

Notwithstanding the positive developments, the RAA observed several shortcomings and deficiencies that require further improvements. In particular, the system objectives were not achieved as the IT systems were either not optimally utilised or did not cater the needs of the users, in other words they do not adequately support RMA's business operations. Apart from this, there were inadequate IT controls in the selected IT systems.

These lapses were largely caused by the IT systems and policies being in its early stage of implementation. The RAA has provided four recommendations to address the weaknesses and implement strong controls in order to render the IT systems effective and credible. Further, INR & CC and AMC system being online is more vulnerable to threats from both insiders as well as outsiders with potential risk to the security of the system.

The RAA hopes that RMA will make further improvements to the system, design and implement IT controls and mechanisms for efficient and effective business operations considering that RMA has spent time and effort to leverage ICT and develop the IT systems.

APPENDICES

Appendix I - Details of Standalone Authorized Money Changers without trade license					
Sl. No	Name of AMC	location	Registered at DoT	Registered at RMA	Registered both with DoT and
1	Bhutan Money Exchanger	Thimphu	yes	yes	yes
2	Shearee Square Money Changer	Thimphu	no	yes	
3	K.C Handicraft	Paro	no	yes	
4	Druk Money Changer	Thimphu	no	yes	
5	H & Q Bhutan	Thimphu	no	yes	
6	LhenTshog Handicraft	Thimphu	no	yes	
7	jitssen Authoirized Money Changer	Thimphu	yes	yes	yes
8	Bhutan Xchanger	Thimphu	yes	yes	yes
9	Tandin Money Changer	Thimphu	yes	no	
10	Sonam Authorized Money Changer	Paro Air port	yes	no	
11	ST Authorized Money Changer	Paro Town	yes	no	
12	TK authorized Money Chnger	Paro Town	yes	no	
13	National Handicraft Eporium	Thimphu Town	yes	no	
14	Jigme Thubten Money Exchanger	Paro Town	yes	no	
15	Money Change Service	Thimphu Town	yes	no	
16	Tashi Authorized Exchanger	Paro Town	yes	no	

Appendix II - List of Money Exchangers without valid AMC license from RMA			
sl. No	**Name of Agent**	**license number**	**Activities**
1	Bhutan Money Exchange	1029615	Hotel license of Wangdue Phodrang, Tabiting
2	K.C Handicraft	1006096	Inactive License Number
3	Druk Money Chnager	R108459	Retail License
4	H and Q Bhutan	1037010	Tours and Travels Agent
5	Lhentsog Handicraft	R1007330	Retail License
6	Jitssen Authorized Money Chnager	1039818	Money Changing Business
7	Bhutan Xchanger	1040840	Money Changing Business
8	Shaeree Square Authorized Money Chnger	nil	No license Number

Appendix III - List of Tourist Hotel with/without AMC license from RMA			
Sl. No	Name of Hotel	Location	AMC License Issued by RMA
1	Village Lodge	Bumthang	no
2	Mountain Resort	Bumthang	no
3	Aman Kora	Bumthang	no
4	Jakar Village Lodge	Bumthang	no
5	Valley Lodge	Bumthang	no
6	Hotel Yu-Gharling	Bumthang	no
7	Gongkhar Guest House	Bumthang	no
8	Jakar View Guest House	Bumthang	no
9	Rinchenling Lodge	Bumthang	no
10	River Lodge	Bumthang	no
11	Swiss Guest House	Bumthang	no
12	Wangdicholing Lodge	Bumthang	no
13	Chhume Nature Resort	Bumthang	yes
14	Hotel Peling	Bumthang	no
15	Kaila Guest House	Bumthang	no
16	Hotel Mipham	Bumthang	no
17	Yoezerling Guest House	Bumthang	no
18	Ugyenling (BTCL)	Bumthang	no
19	Dekyil Guest House	Bumthang	no
20	Ogyen Choling Heritage House	Bumthang	no
21	Tashi Namgay Grand	Chukha	no
22	Hotel Ga Me Ga	Chukha	no
23	Hotel Druk	Chukha	no
24	Lhaki Hotel	Chukha	no
25	The Park Hotel	Chukha	no
26	Hotel Gadhen Namgayling	Chukha	no
27	Hotel Legphel	Chukha	no
28	Hotel Alem	Chukha	no
29	Hotel Palm	Chukha	no
30	Hotel Amochhu View	Chukha	no
31	Soenam Zhingkha	Haa	no
32	Hotel Lhayul	Haa	no
33	Hotel Risum	Haa	no
34	Hotel Wangchuk	Mongar	no
35	Trogon Villa	Mongar	no
36	Bhutan Spirit Sanctuary	Paro	yes
37	Le Meriden Riverfront	Paro	yes
38	Amankora Resort	Paro	no
39	Hotel Zhiwaling	Paro	yes
40	Uma Resort	Paro	yes
41	Heven Resort	Paro	no
42	Six Senses	Paro	no
43	Himalayan Keys Forest Resort	Paro	no
44	Naktsel Resort	Paro	no
45	Basecamp	Paro	no
46	Kitchu Resort	Paro	no

Appendix III - List of Tourist Hotel with/without AMC license from RMA			
Sl. No	Name of Hotel	Location	AMC License Issued by RMA
47	Mandala Resort	Paro	no
48	Metta Resort	Paro	no
49	Reven's Nest	Paro	no
50	Tashi Namgey Resort	Paro	no
51	Hotel Drukchen	Paro	no
52	Hotel Gangtey Palace	Paro	no
53	Hotel Olathang	Paro	yes
54	Khangkhu Resort	Paro	no
55	Tenzingling Resort	Paro	yes
56	Tiger Nest Resort	Paro	no
57	Udumwara resort	Paro	no
58	Rema Resort	Paro	no
59	Paro Village Lodge	Paro	no
60	Hotel Dewachen	Paro	no
61	Janka Resort	Paro	no
62	Namsey Chhoeling Resort	Paro	no
63	Spirit of Bhutan Resort	Paro	yes
64	Namjo Heritage	Paro	no
65	Taktsang Village Resort	Paro	no
66	Uma Resort	Punakha	yes
67	Amankora	Punakha	no
68	Kuenzangzing Resort	Punakha	no
69	Six Senses	Punakha	no
70	RKPO	Punakha	no
71	Zhingkham	Punakha	yes
72	Meri Puensum Resort	Punakha	no
73	Dhensa Resort	Punakha	yes
74	Damchen Resort	Punakha	no
75	Drupchu Resort	Punakha	no
76	Vara Resort	Punakha	no
77	Hotel Kingaling and Spa (New)	Punakha	no
78	Dumra Farm Resort	Punakha	no
79	Punakha Residency (New)	Punakha	no
80	Khuru Resort	Punakha	no
81	Zangto Pelri Hotel	Punakha	yes
82	The Four Boutique Hotel	Punakha	no
83	Hotel Sonam Gang	Punakha	no
84	Dungsam Trashiling Resort	Samdrup Jongkhar	no
85	Le Meriden	Thimphu	yes
86	Amankora Thimphu	Thimphu	no
87	Taj Tashi	Thimphu	yes
88	Six Senses	Thimphu	no
89	Hotel Ariya	Thimphu	yes
90	Druk Hotel	Thimphu	yes
91	Terma linca	Thimphu	yes
92	Norkhill Boutique Hotel & Spa	Thimphu	yes

Appendix III - List of Tourist Hotel with/without AMC license from RMA			
Sl. No	Name of Hotel	Location	AMC License Issued by RMA
93	dusitD2 Yarkey	Thimphu	yes
94	Dorji Element	Thimphu	no
95	Gyelsa Boutique	Thimphu	no
96	Hotel Gakyil	Thimphu	yes
97	Hotel Pedling	Thimphu	yes
98	Hotel Thimphu Tower	Thimphu	no
99	Khang Residency	Thimphu	no
100	Namseling Boutique Hotel	Thimphu	no
101	Norbuling	Thimphu	yes
102	Tashi Yoedling	Thimphu	no
103	Zone Executive Apartment	Thimphu	no
104	Tara Phendeyling	Thimphu	yes
105	Kisa Villa	Thimphu	no
106	Hotel Migmar	Thimphu	no
107	Hotel Jomolhari	Thimphu	yes
108	Hotel Namgay Heritage	Thimphu	no
109	Bhutan Suites	Thimphu	no
110	Hotel Galingkha	Thimphu	no
111	Hotel Kisa	Thimphu	no
112	Hotel Phuntsho Pelri	Thimphu	no
113	Hotel River View	Thimphu	yes
114	Osel	Thimphu	yes
115	Hotel River Side	Thimphu	no
116	Hotel Bhutan	Thimphu	no
117	City Hotel	Thimphu	no
118	Ramada	Thimphu	yes
119	Hotel White Tara	Thimphu	no
120	Hotel Yeedzin	Thimphu	no
121	Hotel Ro Chog Pel	Thimphu	no
122	Wangchuk Resort (Taba)	Thimphu	no
123	Jambeyyang Resort	Thimphu	yes
124	Peaceful resort	Thimphu	no
125	Zhiwaling Ascent	Thimphu	no
126	Amodhara Hotel	Thimphu	no
127	Kunden Hotel	Thimphu	yes
128	Hotel Drukyul	Thimphu	no
129	Kuenphen Rabten Resort	Thimphu	no
130	Hotel Norpheling	Thimphu	no
131	Dewa thimphu	Thimphu	yes
132	Hotel Lhayul	Thimphu	no
133	Druk Doethjung Lodge	Trashigang	no
134	Druk Doethjung Hotel	Trashigang	no
135	Lingkhar Lodge	Trashigang	no
136	Damphu resort	Tsirang	no
137	Yangkhil	Trongsa	no
138	Wangdi Eco Lodge	Wangdue	no

Appendix III - List of Tourist Hotel with/without AMC license from RMA			
Sl. No	Name of Hotel	Location	AMC License Issued by RMA
139	Punatsangchu Cottage	Wangdue	no
140	Pema Karpo	Wangdue	no
141	Hotel YT	Wangdue	no
142	Dragon Nest Resort	Wangdue	no
143	Amankora Resort	Wangdue	no
144	Gangtey Lodge	Wangdue	no
145	Gakiling Guest House	Wangdue	no
146	Dewachen Hotel	Wangdue	no
147	RKPO	Wangdue	no

Appendix IV - List of individuals issued with more 10,000 INR ATS in the same month			
CID	No. of times INR taken during the same month	Month	INR Amount (Taken during the same month)
12008002566	3	September	30,000.00
10906002341	3	July	30,000.00
10714001136	3	April	30,000.00
10705001446	3	August	30,000.00
10811001450	4	September	21,000.00
12006002634	2	August	20,000.00
11915001915	2	April	20,000.00
11911001138	2	April	20,000.00
11910001787	2	March	20,000.00
11910000837	2	September	20,000.00
11812000866	2	March	20,000.00
11805002502	2	March	20,000.00
11705001440	2	March	20,000.00
11608000213	2	May	20,000.00
11607001792	2	March	20,000.00
11513006292	2	March	20,000.00
11513000446	2	March	20,000.00
11512003841	2	March	20,000.00
11510001292	2	September	20,000.00
11509001437	2	April	20,000.00
11508000118	2	May	20,000.00
11506004712	2	March	20,000.00
11401001165	2	March	20,000.00
11106002200	2	March	20,000.00
11101002038	2	March	20,000.00
11007000781	2	March	20,000.00
11006000751	2	September	20,000.00
11005003231	2	April	20,000.00
10903000925	2	August	20,000.00
10811000521	2	April	20,000.00
10811000070	2	April	20,000.00
10807000420	2	March	20,000.00
10805000156	2	June	20,000.00
10801002339	2	April	20,000.00
10712001831	2	March	20,000.00
10708002140	2	March	20,000.00
10607002094	2	March	20,000.00
10607000563	2	March	20,000.00
10502001176	2	March	20,000.00
10502000835	2	March	20,000.00
10211002754	3	September	20,000.00
10203003447	2	March	20,000.00
10203002594	2	March	20,000.00
10203000870	2	March	20,000.00
10102002500	2	May	20,000.00

Appendix IV - List of individuals issued with more 10,000 INR ATS in the same month			
CID	No. of times INR taken during the same month	Month	INR Amount (Taken during the same month)
10101002426	2	March	20,000.00
10705003938	2	June	17,000.00
10706001515	3	March	16,900.00
11913001497	2	March	16,000.00
11915000257	2	June	15,000.00
10906000936	2	July	14,500.00
11604000690	3	August	11,400.00
11405000637	2	May	11,100.00
11503001552	3	May	11,000.00
10811001450	3	July	10,500.00

Appendix V - List of Individuals issued with more than 30,000 INR ATS in the same month			
CID	No. of times INR taken during the same month	Month	INR Amount (Taken during the same month)
11308000917	8	January	160,000.00
485	3	January	90,000.00
12001003680	2	February	60,000.00
11915000385	2	January	60,000.00
11912001625	2	November	60,000.00
11810001699	2	December	60,000.00
11704000277	2	October	60,000.00
11703000513	2	February	60,000.00
11608002053	2	January	60,000.00
11606001043	2	January	60,000.00
11513001452	2	December	60,000.00
11503000123	2	December	60,000.00
11410007060	2	February	60,000.00
11410005882	2	February	60,000.00
11410001417	2	November	60,000.00
11410000844	2	February	60,000.00
11407001541	2	February	60,000.00
11405001157	2	February	60,000.00
11102001267	2	January	60,000.00
10903000623	2	November	60,000.00
10801001494	2	January	60,000.00
10712001139	2	October	60,000.00
10702000507	2	February	60,000.00
10605001816	2	October	60,000.00
10604000107	2	January	60,000.00
10603000320	2	October	60,000.00
10102001577	2	February	60,000.00
11505003155	2	October	55,000.00
11503002713	2	November	55,000.00
10904003095	2	January	54,000.00
11501002198	2	December	51,000.00
11603002424	2	December	50,000.00
11410010748	2	November	50,000.00
10802001900	3	December	50,000.00
10203005156	2	November	49,500.00
11605000207	2	November	45,000.00
11512004281	2	December	45,000.00
10605002938	2	December	45,000.00
10811001450	5	October	41,000.00
12008000975	2	October	40,000.00
11811000595	2	December	40,000.00
11606000708	2	November	40,000.00
11410008897	2	January	40,000.00
11315000779	2	November	40,000.00
11111000251	3	February	40,000.00

Appendix V - List of Individuals issued with more than 30,000 INR ATS in the same month			
CID	No. of times INR taken during the same month	Month	INR Amount (Taken during the same month)
11206000887	2	January	38,000.00
11906000856	2	October	37,000.00
11315000294	4	November	37,000.00
11906000789	2	December	35,000.00
11513003381	2	February	35,000.00
11503000061	2	January	35,000.00
11109000740	2	January	35,000.00
10702001550	2	December	35,000.00
10703001434	2	November	32,000.00
11510003137	2	November	31,000.00

Appendix VI - Issuance of USD ATS exceeding the USD 3000 quota in one year								
Year	Transaction Date	CID	Name	Passport Number	Currency	ATS Amount	Equivalent Currency Amount	Remarks
2018	18/08/2018	10211002974	DECHEN WANGMO	G033356	USD	1307.00	1307.00	ATS USD 1307 ON CREDITCARD
2018	08/08/2018	10211002974	DECHEN WANGMO	G033356	USD	3000.00	3000.00	ATS
2018	06/01/2018	10605004460	JETSHEN PELZIN	G083164	USD	3000.00	3000.00	ATS
2018	06/01/2018	10605004460	JETSHEN PELZIN	G083164	USD	3000.00	3000.00	ATS
2018	07/03/2018	10802000481	TESIN CHOEKI TOBGYAL	G 084977	USD	3000.00	3000.00	ATS
2018	07/03/2018	10802000481	TESIN CHOEKI TOBGYAL	G 084977	USD	3000.00	3000.00	ATS
2018	04/01/2018	10806002196	SANGAY WANGCHUK	G094976	USD	3000.00	3000.00	ATS
2018	04/01/2018	10806002196	SANGAY WANGCHUK	G094976	USD	3000.00	3000.00	ATS
2018	04/01/2018	10806002196	SANGAY WANGCHUK	G094976	USD	3000.00	3000.00	ATS
2018	04/01/2018	10806002196	SANGAY WANGCHUK	G094976	USD	3000.00	3000.00	ATS
2018	04/01/2018	10806002196	SANGAY WANGCHUK	G094976	USD	3000.00	3000.00	ATS
2018	04/01/2018	10806002196	SANGAY WANGCHUK	G094976	USD	3000.00	3000.00	ATS
2018	04/01/2018	10806002196	SANGAY WANGCHUK	G094976	USD	3000.00	3000.00	ATS
2018	31/01/2018	11211001701	Prakriti Rai	G051948	USD	3000.00	3000.00	ATS on Debit Card
2018	31/01/2018	11211001701	Prakriti Rai	G051948	USD	3000.00	3000.00	ATS on Debit Card
2018	31/01/2018	11211001701	Prakriti Rai	G051948	USD	3000.00	3000.00	ATS on Debit Card
2018	03/09/2018	11312003470	TSHEWANG NAMGAY	G084183	USD	692.00	692.00	ATS USD 692 ON HIS INTT CREDITCARD
2018	01/09/2018	11312003470	TSHEWANG NAMGAY	G084183	USD	2600.00	2600.00	ATS
2018	05/01/2018	11410001570	CHOKI DOLMA	G047174	USD	3000.00	3000.00	ATS
2018	05/01/2018	11410001570	CHOKI DOLMA	G047174	USD	3000.00	3000.00	ATS
2018	23/07/2018	11410003171	CHIMI DORJI NORBU	G105997	USD	1065.00	1065.00	ATS USD 1065 ON HIS CREDITCARD
2018	23/07/2018	11410003171	CHIMI DORJI NORBU	G105997	USD	3000.00	3000.00	ATS
2018	09/04/2018	11410003171	Chimi Dorji Norbu	G105997	USD	635.00	635.00	USD 635 ATS ON CREDIT CARD

Appendix VI - Issuance of USD ATS exceeding the USD 3000 quota in one year								
Year	Transaction Date	CID	Name	Passport Number	Currency	ATS Amount	Equivalent Currency Amount	Remarks
2018	20/02/2018	11410003171	Chimi Dorji Norbu	G105997	USD	1300.00	1300.00	ats usd 1300 to visa international credit card
2018	03/10/2018	11410004061	DENKI LHAMU	G031653	USD	3000.00	3000.00	USD 3000 ATS ON CREDITCARD
2018	26/08/2018	11410004061	DENKI LHAMO	G031653	USD	2000.00	2000.00	ATS
2018	25/12/2018	11410005063	PHUNTSHO WANGMO	G041296	USD	3000.00	3000.00	ATS USD 3000 ON INTT CREDITCARD FROM INTT DEBIT CARD
2018	16/06/2018	11410005063	PHUNTSHO WANGMO	Z017405	USD	1500.00	1500.00	ATS USD 1500 ON INTT DEBIT CARD
2018	17/04/2018	11410005063	PHUNTSHO WANGMO	G041296	USD	1500.00	1500.00	USD 1500 ATS ON DEBIT CARD
2018	06/04/2018	11512003546	DORJI WANGCHUK	G088917	USD	2305.00	2305.00	USD 2305 ATS ON CREDIT CARD
2018	06/04/2018	11512003546	DORJI WANGCHUK	G088917	USD	2305.00	2305.00	USD 2305 ATS ON CREDIT CARD
2018	29/03/2018	11513004068	THINLEY GYELTSHEN	G060789	USD	2310.00	2310.00	USD 2310 FOR ATS ON CREDIT CARD
2018	29/03/2018	11513004068	THINLEY GYELTSHEN	G060789	USD	2310.00	2310.00	USD 2310 FOR ATS ON CREDIT CARD
2018	19/01/2018	11513004660	YESHEY WANGCHUK	G103891	USD	1542.00	1542.00	ATS
2018	19/01/2018	11513004660	YESHEY WANGCHUK	G103891	USD	1542.00	1542.00	ATS
2018	25/08/2018	11704003901	RABTEN WANGYAL	G048814	USD	1403.00	1403.00	ATS USD 1403 ON I NTT CREDIT CARD
2018	23/08/2018	11704003901	RABTEN WANGYAL	G048814	USD	2000.00	2000.00	ATS
2018	03/10/2018	11806000433	PRAKASH RASAILY	G078404	USD	210.00	210.00	USD 210 ATS ON CREDITCARD

Appendix VI - Issuance of USD ATS exceeding the USD 3000 quota in one year								
Year	Transaction Date	CID	Name	Passport Number	Currency	ATS Amount	Equivalent Currency Amount	Remarks
2018	03/10/2018	11806000433	PRAKASH RASAILY	G078404	USD	2790.00	2790.00	USD 2790 ATS ON CREDITCARD
2018	14/09/2018	11806000433	PRAKASH RASAILY	G078404	USD	600.00	600.00	ATS
2018	18/06/2018	EC0301415	RAMOS WILLIAMOR CUBILLO	EC0301415	USD	1450.00	1450.00	ATS
2018	18/06/2018	EC0301415	RAMOS WILLIAMOR CUBILLO	EC0301415	USD	1450.00	1450.00	ATS
2018	18/06/2018	EC0301415	RAMOS WILLIAMOR CUBILLO	EC0301415	USD	1450.00	1450.00	ATS

ANNEXURE

ཨོཾ ། རྒྱལ་གཞུང་དངུལ་ལས་དབང་འཛིན།།
ROYAL MONETARY AUTHORITY OF BHUTAN

RMA/DIA-08/2019-20/ 3025 October 16, 2019

The Deputy Auditor General
Department of Performance & Commercial Audit
Royal Audit Authority
Thimphu.

Subject: Response to Information Technology Systems Audit of the RMA

Dear Dasho,

The RMA would like to thank the RAA and the IT system audit team for successful completion of system audit of the RMA. We have enclosed the responses provided against the number of each observation of the system audit conducted by the RAA for the period January- December 2018.

We would also like to request for an exit meeting to resolve the issues in the presence of the Honb'le Governor before finalization of the report.

We would once again like to thank RAA and the system audit team for their courtesy and professionalism exhibited during the audit period.

Thanking you,

Yours Sincerely,

(Phajo Dorjee)
Deputy Governor

Cc:

1. Ms. Sonam Wangmo, Assistance Audit Auditor General, Performance & System Audit Division, RAA, Thimphu for kind information.
2. Ms. Kinley Zam, Senior Audit Officer, Thematic Audit Division, RAA, Thimphu for kind information.

POST BOX:154,CHHOPHEL LAM, KAWAJANGSA, THIMPHU BHUTAN
TEL# :(+975-2-323110, 323111, 323112, 321699) FAX :(+975-2-322847)
SWIFT:RMABBTBT

Response to the observation on Information Technology Systems Audit by the RAA for the Period January-December 2018

3.1.1 INR & CC system does not generate comprehensive INR and CC inflow and outflow report

The RMA web based system was an initiative taken to capture foreign exchange flows through the commercial banks on real time basis. The RMA had provided mass training to the banks staffs on the system and provided adequate time frame for the banks to shift from manual reporting system to system based reporting. However, it was noted that the transactions reported in the system were incomplete and was not reported on real time basis. Further upon inspection of the banks in 2017 it was noted that it entails extra time and workload for the banks as the system was not integrated to the bank's core system, which was not feasible due to banks security reasons.

As such the foreign exchange flows are currently being compiled partially from the system and remaining from excel reports and will continue until proper solution to capture the comprehensive foreign exchange flows is put in place.

3.1.2 AMC system is not optimally utilized for regulation.

(i) Low transactions record of Hotels and use of AMC online system.

For minimal cash transaction at the AMC's, we would like to inform that advance payment for hotel reservations are remitted directly to TCBs account through banking channel. Further, with the advancement of payment methods (cards, payment gateway), funds are directly credited into the hotel's account with the banks. In the resent years, the RMA has also set up exchange counter at the entry point in Paro and Phuntsholing to facilitate exchange services, whereby majority of the foreign currency are exchanged at the point of entry.

During RMA's annual inspections it was also noted that few of the AMC's were not using AMC online system mainly due to system compatibility with their core system and due to the high staff turnover or transfer of the staff trained by the RMA without training the successor. As such the RMA has upgraded the system in 2018 and has been providing training on the AMCs system at the RMA as well as over the counter during the time of inspection. Further, the RMA will also be carrying our ad hoc inspection henceforth.

(ii) Responded under section 3.2.3 below

(iii) Renewal of AMC license for inactive business

Prior to 2018, AMC licenses were issued for unlimited validity period. In 2018 the MoI was amended incorporating the validity of AMC license (one year) and renewal of the license to be based on the performance/operation of the business. After the amendments, the RMA notified all the AMC (dated 24 April 2018) license holders to renew their existing license and those opting to provide the exchange facility was issued license with validity for a year.

Subsequently, we also conducted inspection of the AMCs located at Thimphu, Paro, Punakha and Phuntsholing from 13 May to 6 June 2019. During the inspection our team reiterated the requirements as per MoI and also informed that the renewal of license will be based on the operation of business and fulfilment of the requirement under MoI.

It was internally discussed that the renewal/cancellation of AMC license will be carried based on the performance/operation of the business for 3 consecutive years and it has only been a year since the implementation of the amendments.

3.1.3 ICBS does not support some core functions of RMA

ICBS system consists of different integrated modules, such as HR, Inventory, Currency and Banking, etc. The system has been enhanced over time, based on the change request, which are mostly related to changes in the accounting policy from GAAP to IFRS. The implementation is still under the transition stage and is expected to be fully compliant by 2022. Till date, the accounting conversion and the related financial reporting were developed compliant with IFRS. Given that the accounting conversion is an on-going process, requiring new requirements and scope to be finalized by the business owners, the existing system will be further enhanced to support new accounting policy. Therefore we would appreciate if the observation can be dropped.

3.2 Lapses in regulation of AMC

3.2.1 (i and ii) Discrepancies between RMA and DoT list of AMC

Section 362 of the FSA states that the Authority may regulate financial services other than banking, insurance or securities business by adopting regulations to establish systems of licensing and regulation consistent with the sections of this Act applicable to financial services, including but not limited to cooperatives, lending companies, Foreign Exchange dealers or money transmitters, and any services which is deemed financial in nature

Further, as per section 14 of the FERR 2018 any person other than authorized bank may apply for a license from the RMA to carry out money changing business in Bhutan. As such, the RMA issues AMC license based on the trade license issued by DoT.

With regard to the requirement of trade license, we are currently verifying the validity of the trade license of all the AMCs registered with RMA.

In the recent AMC inspection, we have also come to notice that AMC license is also being issued by Department of Small and Cottage Industry (DSCI), and those licensed by DSCI is not registered with the RMA. In this regard, we are in discussion with the DSCI to clarify on the authority for issuance of AMC license. Based on the outcome of the meeting we will issue notification advising those licensed by DCSI to register with the RMA. We are also collecting the list of AMC license issued by DCSI and have already registered and licensed few. We have also issued notification notifying those individuals facilitating exchange services without AMC license to register with RMA for AMC license on 28th September 2019.

The RMA will resolve the discrepancy with DCSI; therefore, we request that the observation be dropped.

3.2.1 (iii) Hotels not issued with AMC license by RMA.

AMC license is provided to those individuals opting to provide exchange facility. As such it is not mandatory for all hotels to have AMC license, only those individuals opting to provide exchange facility is required to have AMC license issued by the RMA.

The AMC's are only permitted to buy foreign currency (FC) whereas the banks are permitted to buy and sell foreign currency. To curb illegal FC exchange, the RMA has upgraded the AMC system in 2018, whereby the systems are linked and the cash receipt are system

generated. As such the clients/ tourist selling FC to AMC's can buyback/reconvert FC from the banks exchange counter at exit point upon submission of the system generated cash receipt.

Further, the RMA has also issued notification advising the general public facilitating exchange services to register with RMA for AMC license. We propose to issue such notifications on annual basis and when deemed necessary.

3.2.2 Inadequate supervisions of AMCs.

The RMA has been conducting inspection of the AMCs on annual basis whereby they verify the infrastructure and transactions (reports available). The RMA prior to issuance of license conduct onsite inspection to verify infrastructure and location requirement. Further, we will also be initiating ad hoc inspection henceforth.

3.2.3 Comprehensive information on AMC not captured in the AMC System (Publication of AMCs on the RMA website and AMC system).

We have the updated list of AMC which we continue to update upon renewal of AMCs. We are in the process of reviewing the AMC application form and will be incorporating changes with applicant details where necessary. And as recommended we will host the updated lists on the RMA website and AMC online system for monitoring purpose. Therefore we would appreciate if the above observation can be dropped.

3.3.1 Improper procedures for user account creation

The users are created based on the office memo, specifying rights and privileges, from the head of the department and the same memo is archived for future reference. In order to further streamline the procedures and controls, the department will reinstate template forms, adhering to the principle of least privilege, by the end of December 2019.

3.3.2 Shortcomings in user account management

Currently, the username is created based on the internal naming convention. In few cases, there were shortcomings to adopt the same convention. Those usernames, which are not consistent, will be rectified accordingly.

3.3.3 Weak password management

The passwords are currently masked and stored in unreadable format. In order to further secure the system, a strong password validation will be enforced to the users hereafter.

3.3.4 Access right not updated with change in role and responsibility

Access rights and permission are created based on the request from the department. In few cases, such as during internal staff transfer, the rights and permissions have not been updated accordingly. The department will institute a process wherein any profile change/transfer will be informed to DIT to make concomitant changes in the system. However, the access rights have been updated in the online system. Considering the ratification, we request that the observation be dropped.

3.4.1 Session timeout not set for the system

Session timeout is currently configured at the desktop level, which will automatically log out the users within a predefined idle time. Based on the recommendation, session timeout will be developed and calibrated for each system.

3.4.2 Unlimited unsuccessful logon attempts

The number of unsuccessful logons will be limited to 3 attempts and after that the user will be disabled. It was initially kept open to provide flexibility to diverse users.

3.4.3 Vulnerabilities in INR & CC and AMC system

DIT is currently exploring on conducting comprehensive vulnerability and penetrating testing for the systems accessible via RMA website. The findings will be treated accordingly.

3.5.1.1 Invalid Names and contact numbers

The names field will be developed to accept only alphabets and the contact numbers to accept only numeric digits by December 2019.

3.5.1.2 Invalid CID numbers

The current system design accepts CID less than 11 digits since there are cases wherein we have to release INR to different card holders, such as special resident permits having different CID length. Nevertheless, we will incorporate a new field for special permit number and CID field will be restricted to accept 11 digits.

3.6.1 INR issued more than allowable limit

We will enforce strict validation in the system to check the limit for INR without exception to the rule. Further, we will train the end users on how to check the limits and input the requisition. In some cases, the reasons could be attributed to the Internet connectivity issues wherein the users tend to save same record multiple times by clicking on save button.

3.6.2 USD ATS exceeded the quota

We will enforce strict validation control to check the quota limit. However, in some cases, the reasons could be attributed to the Internet connectivity issues wherein the users tend to save same record multiple times by clicking on save button.

3.6.3 INR system accepting amount below the minimum amount

As per Foreign Exchange Operational Guidelines 2018, Annex II, the total ATS per month is 10,000/. There are no provisions where it states that the minimum INR amount to be issued should be INR 500. Therefore, this observation can be dropped.

3.6.4 INR and CC system contains list of countries where INR is not required

Destination such as Sri Lanka and Tibet are also listed in the system because we consider the final destinations of the travel. The INR is issued for such destinations if the travel is routed via India for on route expenses. Considering the above response, we request that the observation be dropped.

3.7 Improper segregation of incompatible duties of ICBS

ICBS design is based on maker- checker concept, consisting of creator, verifier and authorizer. While it's the responsibility of the concerned department to segregate functional duties, the DIT will make concerted effort to enforce maker-checker principle.

3.8 Lack of adequate surveillance in the systems

Currently, the system logs transaction details, timestamp and user ID. Based on the recommendation, the logs will be further reviewed to capture end-to-end trails and will timely monitor the logs.

3.9 User training not provided

As mentioned above, we will train the end users on how to check the limits and input the requisition for INR & CC system. Additionally, we will also provide user training for all other system.

3.10 Lack of Business Continuity Plan

Database backup is performed daily at the primary site and stored at the primary and Phuentsholing backup site.

3.11 Inadequate system documentation

System documentation pertaining to ICBS, such as the software requirement specification, design document, minutes and memos are available for reference.

RECOMMENDATIONS

4.1 RMA should ensure that the IT systems developed are used for intended purpose

- ✓ RMA will ensure that AMC system is used by all Authorized Money Changers by end of December 2019.
- ✓ As such the foreign exchange flows are currently being compiled partially from the system and remaining from excel reports and will continue until proper solution to capture the comprehensive foreign exchange flows is put in place since this initiative involves external stakeholders(banks).
- ✓ ICBS system caters to all the core business functions, however, the accounting conversion is an ongoing process, requiring new requirements and scope to be finalized by the business owners, the existing system will be further enhanced to support new accounting policy.

4.2 RMA should institute robust IT controls in ICBS, INR & CC and AMC systems

- ✓ RMA will institute and enforce robust IT controls in the systems particularly in the areas recommended by the RAA. All of the recommendations will be implemented by end of December 2019.

4.3 RMA should institute mechanism to enhance management of Authorized Money Changers

- ✓ As recommended the RMA will host the updated lists on the website and AMC online system for monitoring purpose.
- ✓ Based on the outcome of the meeting we will issue notification advising those licensed by DCSI to register with the RMA. We are also collecting the list of AMC license issued by DCSI and have already registered and licensed few. We have also issued notification notifying those individuals facilitating exchange services without AMC license to register with RMA for AMC license on 28th September 2019.
- ✓ RMA are in the process of reviewing the AMC application form and will be incorporating changes with applicant details where necessary including MOI.
- ✓ RMA will also be initiating ad hoc inspection henceforth.

4.4 RMA should enforce proper segregation of duties

- ✓ While it's the responsibility of the concerned department to segregate functional duties, the RMA will make concerted effort to enforce maker-checker principle.

རྩིས་ཞིབ་ངོ་རྟགས་ཨང་: ༡༦༡༨༢

AIN: 16182

www.bhutanaudit.gov.bt