National Audit Office Malawi

Report on Fraud and Mismanagement of Malawi Government Finances

Covering transactions and controls in the six month period 1 April 2013 - 30 September 2013

Report dated 21 February 2014

Contents

Baker Tilly Business Services Limited

Abbreviations

Detailed descriptions and explanations of terms and abbreviations relevant to this report are listed below. These descriptions and explanations serve to clarify our report and are not intended to be authoritative.

Abbreviation	Description
ACB	Anti-Corruption Bureau
DFID	Department for International Development
FIU	Financial Intelligence Unit
GoM	Government of Malawi
GRN	Goods received note
GWAN	Government Wide Area Network
IFMIS	Integrated Financial Management System
IMF	International Monetary Fund
MK	Malawi Kwacha
NAO	Malawi National Audit Office
ODPP	Office of the Director of Public Procurement
ORT	Other Recurring Transactions account
PFMA 2003	Public Finance Management Act
PV	Payment Vouchers
RBM	Reserve Bank of Malawi
Soft-Tech	Soft-Tech Consulting Limited
TI 2013	Treasury Instruction 2013
UK	United Kingdom

1. Executive Summary

1.1. Introduction

Baker Tilly Business Services Limited (Baker Tilly) currently holds a framework contract to provide forensic and investigation audit services to the United Kingdom's (UK) Department for International Development (DFID). In October 2013 Baker Tilly was asked by DFID to provide forensic and system security audit services support to the Government of Malawi (GoM) following the discovery of irregularities by staff of the Accountant General during a routine examination of the Budget Exception Report. Further in-house investigations by the Accountant General revealed that significant amounts of government money appeared to have been misappropriated. The incident is widely referred to in the Malawi media as the 'Cashgate' scandal.

In response to these apparent irregularities, the GoM instructed a thorough forensic audit of suspected misappropriations for the months April to September 2013 to be completed to ascertain the facts behind these allegations. At the time of the request these misappropriations were understood to involve between 8 and 10 Ministries.

This report provides our findings and observations relating to the control framework from our first tranche of work. A further report will be provided to the Auditor General on completion of the IT Security element of our work.

1.2. Background

In 2005 the GoM appointed Soft-Tech Consulting Limited (Soft-Tech), an EPICOR Ltd software solutions technology partner, to implement an EPICOR based Integrated Financial Management Information System (IFMIS) for supporting budgeting, accounting and reporting. Over recent years the GoM has customized IFMIS to meet its own specific requirements across 50 Ministries and government entities. IFMIS generates payments to suppliers entered onto the system. In turn cheques are raised for payment to suppliers and others which are then printed on Reserve Bank of Malawi (RBM) cheques. This function is currently centralized at the Accountant General's Department. All the payment vouchers, less the supporting documents from the various Ministries, are manually brought to the Accountant General's Department for verification before cheques are processed.

The IFMIS system is designed to enable the GoM to monitor its budget and cash position. However subsequent reviews have identified significant control weaknesses within the system. The GoM suspect that a number of perpetrators have exploited these weaknesses through collusion, resulting in financial loss to the government exchequer. In the latest episode, it is alleged that the perpetrators were able to transfer funds from the government bank accounts to the vendor accounts for goods and services that were never supplied and then to delete these transactions from the IFMIS system. It is

claimed that the system was manipulated to release funds without lawful authority, create and approve unauthorized payments, issue cheques through the Accountant General's Department and transfer funds into supplier accounts without authorisation.

The preliminary audit work completed by the GoM revealed that, within IFMIS, a significant number of transactions had been deleted. To quantify the extent of these deletions and identify how the internal control failures occurred, the Accountant General commissioned Soft-Tech to complete an investigation.

The outputs of the Soft-Tech report have been relied upon to inform our work.

At the same time the Auditor General instructed that this review be undertaken and that this should include deleted transactions.

This report is supported by case files pertaining to individuals or companies where questionable transactions and potential criminal activity has been identified and have been referred to the relevant Law Enforcement Agencies.

1.3. Scope of the Review

The Baker Tilly review team has operated in Malawi since commencing the assignment. During this period we have interacted with key stakeholders including the Auditor General, Accountant General, RBM, Soft-Tech, Anti-Corruption Bureau (ACB), Financial Intelligence Unit (FIU), the Police, the International Monetary Fund (IMF) and a number of interested donor and Ministries' representatives. Various stakeholders are represented on the Reference Group, chaired by the Auditor General, which was formed to share information, to enhance uniformity and to limit any duplication of investigation work.

The agreed scope of the work required us to:

- Follow the money in various bank accounts through which funds may have flowed;
- Identify all entities that may have received such funds, including vendors who may have been paid without supplying legitimate goods and services, and in case of businesses, their owners, shareholders, directors, etc;
- Identify, if false, forged or fraudulent supporting documents and accounting entries in the books and records (including IFMIS) of Ministries;
- Identify, quantify and evidence alleged misappropriated funds;

- Provide factual information that can be utilized in support of any possible litigation process to re-claim funds that were inappropriately paid during this period, as well as for any civil or criminal prosecution of entries involved, if the government so decides;
- Identify failures and weaknesses in internal controls, including failures within procurement system, that led to these breaches and provide recommendations and suggested actions to strengthen controls and mitigate future risks; and
- Provide suggested actions to strengthen any other procedures as may be agreed.

We have undertaken work to understand the position of the GoM bank account structure and how these accounts link to the Ministries. The audit team has also extracted IFMIS data for further interrogation and profiling and worked with the relevant law enforcement agencies to understand how they are completing their investigations.

The audit did not focus solely on the deleted transactions identified in the Soft Tech report but extended its scope to consider payments made through the Governments main 11 bank accounts includingMG1.account, and included selecting a sample of those transactions for further testing. It did not consider the other 529 accounts held by the GoM.

Our initial data assessment considered the bank account statements for the period July 2012 to September 2013, profiling a total of 368,526 transactions. This data allowed the audit team to consider patterns and trends of deposits withdrawals and adjustments to inform the transaction selection for the auditable period of April 2013 to September 2013. Where available, and appropriate, the period for October 2013 has also been included.

A further risk assessment was undertaken based on selected criteria; this assessment identified a judgemental sample of 501 transactions. We obtained cheque images for these transactions and collected data and evidence to allow a secondary risk assessment to be undertaken. The transactions, identified in the Soft-Tech report as deleted from IFMIS, were also considered.

The audit trail for each transaction has been recreated by tracing the corresponding IFMIS cash book entry, obtaining scans of the signed cheques identifying the cheque signatories and locating any third party supporting documentation.

A review of the IFMIS deleted transactions has been completed and matched against payments made from the GoM bank accounts. It should be noted that not all of the deleted transactions have been cleared through the banking system and therefore some remain unpaid.

1.4. Summary of Findings

The work performed to date, and this report, focus on the period 1 April 2013 to 30 September 2013. This report is based on our findings and specifically the completed reviews of transactions we believe to meet similar criteria to that identified in the deleted transactions or considered to be higher risk based on our selection criteria. We consider that our work has included all lines of available supporting evidence. It is therefore our view that any figures quoted in this report as discrepancies or monies that have been misappropriated are quite likely to change on further investigation and as more cases complete.

With the exception of specific work on the deleted transactions, the sample we selected for detailed investigation was not based on criteria such as company, Ministry or individual but based on high values and payments of the same value made more than once. We adopted this position to ensure that our work did not focus solely on the deleted transactions.

To limit the risk of prejudicing any current or future legal action, this report does not comment on specific transactions, names or companies. Where we believe fraud, theft or unethical actions have taken place, these have been and / or will be referred to the relevant Law Enforcement Office of the Police and Anti-Corruption Bureau through the Office of the Auditor General.

We have obtained evidence from the various core sources rather than rely on any third party source, we have requested subpoenas/court orders and rebuilt the audit trail. The complexity of some of the cases required tracing funds through multiple related bank accounts, many of which were previously unknown. It should be noted, however, that we believe that additional work is required to complete the remaining case files.

Based on our work we consider that funds have been stolen from the GoM through a variety of means. We believe there are at least two methods being used.

The first method focuses on extraction of ‘cash’ (with the main currency being that of Malawi Kwacha) using systematic money laundering activities through commercial organizations This method would appear to be premeditated, planned and was not opportunistic. We noted a number of companies opening new bank accounts two or three months prior to the receipt of government cheques. For other payments, cheques were paid into the bank accounts of companies who were either dormant prior to payment or showed limited transaction activity through the bank account. We believe these payments relate to the ‘Cashgate’ allegations which led to the request for this review to be undertaken. As of 20 February 2014 we can confirm that up to MK 6,096,490,705 could currently be classified as theft of

Government Funds and subject to appropriate legal action. We believe this figure will continue to change as we review more cases.

The second method identified is, we believe, separate to the 'Cashgate' affair and may be part of a wider corruption scandal that focuses on overvalued and high value transactions, payment for goods not received and funding transferred internationally to overseas jurisdictions into foreign currencies such as USD and SAR.

A preliminary review of the deleted transactions has been completed and a total of 598 entries have been found to have been deleted from the IFMIS system using the User ID of four individuals.

At the time of this report our findings have identified payments to 16 companies valued at MK6,096,490,705 where no evidence has been provided to support the provision of goods or services in relation to the payment made as such MK6,096,490,705 should be classified as theft of Government Funds and subject to appropriate legal action.

In addition we have identified high value payments made to two newly formed companies. The contracts awarded, if compared to international external price verification resulted in MK 3,619,539,979.20 at best being spent inappropriately or at worst, being stolen.

We found that additional payments totalling MK 3,955,366,067.19 had then been made to the same two companies. At the time of this report no supporting evidence has been provided in relation to these payments. In the absence of suitable evidence consideration should be given to immediate further investigation of those involved in the approval of these payments. This may lead to charges being made against the individuals concerned.

This table summarises the different types of misappropriation.

No.	Type	Amount MK	Amount %
1	Cashgate transactions	6,096,490,705	45%
2	Payments with no supporting documents	3,955,366,067	29%
3	Inflated procurement prices	3,619,539,979	26%
		13,671,396,751	100%

It should be noted that:

- the on-going nature of this investigation and the desire to issue this report would suggest these figures are likely to increase as more cases are reviewed;
- the cashgate figure relates to the six month period April to September 2013; and
- figures relating to unsupported and poor procurement include transactions covering the periods 2012 to 2013.

During our fieldwork we noted significant sums of Malawi Kwacha withdrawn in cash (often significantly higher than the cash holding insurance limits of the commercial banks) in short periods of time from the commercial banks; it appears that the banking system failed to identify these unusual transactions with a limited number of Suspicious Transaction Reports being sent to the FIU. We believe that these levels of withdrawals would increase the cash calls that should have been identified as unusual by the banks and Reserve Bank. Thus, in our opinion, more stringent legislation and investment should be considered in order to strengthen the powers and capacity of the FIU.

The amount of stolen funds extracted in the form of cash withdrawals into Malawi Kwacha would further suggest significant sums have yet to be recovered by the Malawi law enforcement agencies.

Overall, we have identified funding misappropriation and theft of GoM funds. We have seen funds transferred between unrelated companies, individuals withdrawing funds from unconnected organisations and inflated prices paid to companies with limited or no trading history and very large cash withdrawals. We do not believe the receivers of these funds are therefore the ultimate beneficiary in all cases. However, in our opinion further specific detailed work is needed to support the Malawi Law Enforcement Agencies in investigating these matters across international jurisdictions. In this regard we encourage the international donors to continue to support oversight and thus to support on-going investigations in order to ensure convictions and, if possible, reparations.

Our comments relating to control failures relate to the period of time during which our audit team observed, assessed and tested compliance with those controls. We understand, since that time, that some remedial action has commenced; as such some of the recommendations set out in this report may already have been implemented, although we have not undertaken any work to verify the completeness or efficacy of implementation.

The RBM operates under Law Chapter 44:02, one of its principal objectives being Part III 4 (b) *'to act as banker and advisor to Government',* the 'advisor' element suggesting active not passive involvement in managing client funds' availability.

We note the MOU at 10.1.2 (2) states that '*the Bank in collaboration with Government shall ensure no fraudulent cheques are cleared in the system'*. We have particular concerns that high value cheques, including those with exact values on consecutive cheque numbers, were withdrawn on the same day. No evidence has been provided to show that these payments were, at any stage, challenged. We believe these high value transactions could have been stopped were they subjected to more robust secondary checks.

We were unable to identify any audited financial statements relating to individual Ministries, unless they have been specifically required and undertaken on behalf of individual donors. Evidence has been provided, by the National Audit Office, of external audits being undertaken on the consolidated government account. We note that the audit of the financial statements for Individual Ministries has now commenced and welcome this fact.

Significant control failures and lack of application of the existing controls are key factors contributing to the failures and to the theft and misappropriation of funds. The lack of accountability allied to a failure to apply or detect compliance with the Public Finance Management Act (PFM) requirements, has allowed what could be considered to be deliberate circumvention of the control framework that existed at the time. The apparent level of collusion and circumvention, together with limited challenge by those charged with accountability and lack of detailed external audit, would suggest that there is no guarantee or assurances that future occurrences would not happen regardless of any control improvements implemented.

1.5. Limitations

This report does not indicate which individuals or companies are involved in any of the potential frauds identified. This has been done deliberately to limit the risk that we will prejudice any on-going or future legal proceedings. The specific details of these have, or will be, referred to the relevant Law Enforcement Agency. Where appropriate we have included reference to the values at risk based on the evidence provided and seen.

The findings expressed in this report are based on the documents and explanations provided to us. Should further information become available, we reserve the right to modify our findings where necessary and acknowledge that we have a duty to do so.

Insofar as this report refers to matters of law, it should not be taken as expressing any formal opinion whatsoever.

This report is based on the facts established from documentation provided by the various representatives of the GoM, RBM, various commercial banks, individuals and funding recipients

interviewed. Where appropriate we have made reference to additional information and explanations obtained during the course of this review.

We have accepted the various documents provided for what they purport to be and we did not enquire into their authenticity unless we had cause to do so.

Our assessment is based on the documents provided by representatives of the various Ministries and Departments of the GoM, RBM, various commercial banks, individuals and funding recipients interviewed. Electronic scanned copies of original documents are available should they be required.

There are documents and information that may exist which we have been unable to locate, which were not handed to us or were not provided in the time that was available to us.

As part of the audit methodology, sampling techniques have been used and as such we cannot provide assurance that the procedures applied will have detected all potential anomalies or irregularities.

Neither Baker Tilly nor any of the entities within the Baker Tilly Group acts as accountant or statutory to any party involved in this review. Except where specified, we have carried out no audit or verification work in relation to the information on which we have relied. This review does not constitute a statutory or external audit of the records maintained by any party.

The focus of our work related to the funds managed by the Government of Malawi, unless necessarily required otherwise.

The audit sample of 501 transactions has been selected based on our risk criteria and does not include all transactions that the GoM processed between April and September 2013.

With the exception of the Baker Tilly team we are not aware that any other members of the Reference Group have signed the agreed confidentiality agreement presented to the Reference Group to limit disclosure of information during the audit process.

We have requested confirmation from the relevant bodies that all information has been provided. Where no response or communication is received we have assumed that it is complete. To date not all requested information has been provided by the various bodies with whom we interacted.

1.6. Procedures Performed

We obtained the electronic bank data for the GoM's main bank accounts with particular reference to those linked to the deleted transactions. We profiled the income and expenditure over the six month period selected for review to gain an understanding of the profile of Government spend and to identify high risk areas to target. This exercise was complemented by an analysis of the 2012/13 approved estimates of expenditure for the recurrent and capital budget for the Government in order to identify the relative size of each Ministry or Department's budget.

The electronic bank data for the Government's main bank accounts was extracted from the RBM financial system by RBM staff under the supervision of members of the audit team.

The electronic bank data extracted covered an 18 month period, and included the following GoM bank accounts; Malawi Government Account Number 1 (MG1), Development Phase II account, Other Recurrent Transactions Account, Statutory Expenditure Account, Advances Account, Deposit Account, the Accountant General – Northern Region Other Recurrent Transactions Account, the Accountant General - Southern Region Other Recurrent Transactions Account and the Accountant General - Eastern Region Other Recurrent Transactions Account.

We were initially provided with bank statements by the RBM in electronic format whose extraction was not independently supervised by the audit team. In addition we requested extraction of the same data under supervision. A comparison exercise was undertaken between the unsupervised and supervised statements noting a small number of transactions missing between the two datasets and differences in the opening and closing balances.

A review of the electronic bank data extracted under supervision was completed and two types of transactions selected for the test sample; all payments greater than MK 90m and duplicate payments of value between MK 12.5m and MK 90m. Emphasis was placed on these types of transaction to enable us to better understand how the Government spent the majority of its funding and to look for possible duplicate payments, the latter being common indicators of potential misuse of funding. This exercise identified a significant number of bounced cheques, adjusted, reversed and duplicated transactions.

This sample (referred to henceforth as the '501 sample') included a number of different types of payments including cheque withdrawals, cheque deposits, and foreign currency transactions. A number of these payments are the aggregated total of a number of smaller payments.

Documentary evidence to support the payments was obtained from the RBM including images of the front and backs of cheques from the bank's information hosting system as well as cheque signatory

information. A number of the transactions selected were electronic fund transfers or adjustments and, although cheque images were not available, other supporting documents were provided by different departments within the RBM. Where possible screen shots of transactions were also taken to provide a complete audit trail showing which bank employees had reviewed, approved and authorised the payments. A similar exercise was undertaken for the deleted transactions identified by Soft-Tech.

Information was obtained from the FIU; ACB and Police. The FIU provided monthly spread sheets showing large payments and international electronic funds transfers by the majority of the Malawi commercial banks.

To support the audit sample matching cashbook and other associated reports were extracted from the GoM's financial system, IFMIS. Extracts were obtained of the cashbooks for all the relevant Government Ministries and Departments for the two financial years relevant to our sample (2012/13 and 2013/14). Our request for unrestricted user account access met with unnecessary delays impacting on our planned timetable.

The Office of the Director of Public Procurement (ODPP) provided a comprehensive list (in contract number order) of all of the contracts for goods, services and works approved by the ODPP since July 2012 to date. The information provided included the procuring entity, method, date, item, description, value, supplier and contract type.

Based on a judgemental sample of the 501 transactions we identified 352 transactions of interest informed by factors such as value, company name, date of transaction, payment method, and bank.

Working with the commercial banks we obtained bank account opening documents (bank mandates), bank statements and, where necessary, cheque scans or other supporting documents. 11 commercial banks in Malawi were visited and served initially with letters, and later subpoenas, from the NAO requesting this data. The audit sample also included payments to a number of international banks who reside outside the legal jurisdiction of Malawi and have therefore not been contacted to provide information.

The information collected supported the development of a comprehensive database to track payments from IFMIS through the RBM to the commercial bank. The database includes the signatories of the original Government cheque, the recipient company and the bank account where the funds were paid in to. In the majority of cases for the deleted transactions funds have been withdrawn from the company bank accounts and supporting cheques and evidence of the individuals who withdrew the cash has been obtained.

We visited various Government Ministries and Departments to try and obtain the invoices, receipts, contracts and other supporting documents provided by suppliers. In instances where no supporting information could be provided the suppliers of the goods, services or works were visited and asked to provide the necessary paperwork justifying why they had received Government funds.

Interviews were undertaken and supporting information was requested from various suppliers.

We worked closely with the Malawi Revenue Authority to confirm imports of goods into Malawi.

1.7. Report

Upon delivery of this report to the Auditor General, the Auditor General will assume responsibility for the report.

2. Findings: Control Environment

2.1. Introduction

Organizations usually operate three lines of defence to protect their assets; the lines of defence can be simplified as

- Operational Management and internal controls, those being the staff, management, regulations;
- Compliance, risk management and secondary review including that expected of the Accountant General's Department; and
- Internal and external audit and other statutory bodies, this includes the commercial and Reserve Banks.

The failure of these three lines to operate effectively, either collectively or in isolation has, in our view, contributed to the 'Cashgate' opportunity.

2.2. Accountant General's Department / Financial Management Controls

Two Accountant Generals were in post during the period of our sample. The previous Accountant General held the position between 1 June 2013 and December 2013, another Accountant General held the post prior to June 2013. The current Accountant General took up post in December 2013.

The audit team was provided with contradictory information regarding the role and responsibilities of the Accountant General and we have therefore applied the roles established in the Treasury Instruction (TI) (1 May 2013) and Public Finance Management Act (PFM) (No7 of 2003) when assessing the expected roles and responsibilities of the Accountant General, including assessing the elements of the control framework which should be the responsibility of the Accountant General.

Various barriers were noted on commencing our work at the Accountant General's Department. These included delays by the IT department in providing full read only access to IFMIS. Hard copy bank statements for the main GoM bank accounts were also not available for review and poor filing initially made identifying these accounts difficult.

At the time of the commencement of our audit we noted significant failures in the control environment encountered at the Accountant General's Department. Basic accounting procedures and protocols, including those required by the TI and PFM Act, were not being followed or applied. A lack of oversight, accountability and individuals who were 'unchallengeable' by juniors has provided opportunity for a higher level of loss than had the prescribed controls been implemented.

We noted that cheques brought to the Accountant General were signed without proper or adequate review and without checks being made regarding the values, purpose of the payment. When

challenged it was stated by the Assistant Accountant General that, under the current review process, payments were authorised and reviewed by two other authorised signatories before the cheque was signed and therefore it was unnecessary for any further review. The roles of the Accountant and Assistant Accountant General in the final approval process are an essential part of the final government check functions. We therefore draw the Accountant General's team attention to the TI and PFM Act. '*As authorizing officer the Account and Assistant Accountant Generals are a key element of the control process and are as noted below liable for the approvals made and therefore the payments made'*.

We understand that all cheques payments over MK 2, 000,000 (previously MK 5, 000,000 prior to Cash-gate) require three signatures to allow the Reserve Bank Malawi to process payment. In our sample of 352 transactions, 18 transactions with values between MK 13,146,500.00 and MK 209,490,311.20 contained only two signatures. All were honoured by the RBM.

50 transactions in our sample required signature, 32 were signed by the Accountant General between June and September 2013 with a value of MK 16,035,406,948. This includes 14 cheques found on the deleted transactions list with a value of MK 424,645,192.40.

Between March and September 2013 our sample identified 240 cheques signed and approved by the Assistant Accountant General to the value MK 40,008,478,560 including 28 found on the deleted transaction list (value MK 2,666,346,993).

In the majority of cases we noted limited supporting documentation (with the exception of IFMIS generated documentation) to support the deleted transactions. This was confirmed by suppliers interviewed. This would suggest that no documentation was available and checks had not been undertaken correctly to verify the payment. As per TI 5.26.1 '*Payment for goods and services received shall be effected upon verification and confirmation that goods were received or that those services were rendered. Payment shall be made where, a copy of the local purchase order, an invoice and goods received note are attached to the payment voucher.'*

Both the Accountant and Assistant Accountant General at the time of 'Cashgate', as well as the Accountant General in post prior to their appointment, could be considered to have failed in their public duties by not challenging and checking the validity of the payments they have approved thereby contributing to the loss of government funds. That said it should be noted that the previous Accountant General identified the deleted records resulting in the 'Cashgate' enquiry within five months of his appointment.

The Government should consider enforcing TI 5.26.8 In the event of any incorrect payment being made; '*the authorizing officer shall be personally liable and shall be surcharged in respect of any such incorrect payment'*. We are not aware of this clause being enforced, although it is set out in the Treasury Instructions.

We noted that key individuals in the Accountant General's Department, including those who can be seen to be accountable for approving the unsupported payments, have since been redeployed to other Ministries.

Value limits for approval of expenditure by Controlling Officers (senior officers) are, in our view, inappropriate. Currently requirements are for thee signatures on values over MK 2,000,000. We recommend that all payments for expenditure over MK 10,000,000 should be approved by the responsible Principle Secretary not the Controlling Officer.

Any sound control system should operate a range of compensating (often detective) controls designed to work together to identify or prevent loss should one or more controls fail. Unethical and incorrect transactions are often identified through a series of compensating controls designed to limit abuse. These include, but are not limited to, segregation of duties, bank reconciliations, accountability for budgets, adherence to authorization levels, physical checks and verification. These controls are supplemented by external checks, such as those by the banks or FIU and through oversight functions such as external audit.

A review of the TI and PFM Act would suggest that adequate controls are considered and have the basis to be effectively implemented; however they do not appear to operate in practice. There is no incentive to challenge unethical behaviours with key checks and balances not operating, disregarded or removed. This serves to increase the opportunity for manipulation and abuse.

At the time of our review, monthly bank reconciliations had not been completed by the Accountant General's Department for since April 2012. TI 2.4.11 states a responsibility of the Accountant General is the 'Reconciliation of Malawi Government Control Account Number I and all related operating bank accounts maintained at the Reserve Bank of Malawi.' This had also not been undertaken by either of the previous Accountant Generals or flagged as a control issue by the Auditor General. Bank reconciliations represent the most basic and, at the same time, most fundamental of financial controls. Failure to complete them is therefore of significant concern.

Bank reconciliations are an important and basic check to reduce the potential for accidental or deliberate errors. In their absence, no assurance can be provided that the bank transactions have been recorded correctly in the GoM records. Monthly preparation of bank reconciliations also assists in

the regular monitoring of the cash flows of an organization. We are concerned that the consensus, including from qualified accountants in the Accountant General's Department, is that bank reconciliations were not undertaken as they could only be undertaken in IFMIS. This suggests a limited understanding of how and why bank reconciliations are undertaken and an underestimation of their importance in the control framework.

We understand that attempts to automate bank reconciliations through IFMIS are on-going though these have encountered setbacks with opening balances and balances on accounts provided by RBM not matching. We would suggest that manual reconciliations are undertaken unless and until there is adequate IFMIS capability.

The audit team witnessed the preparation of GoM cheques in the corridors of the Accountant General's Department and blank cheques left in printers overnight, though this was not routine it does suggest that classified financial information and security documents are not adequately respected or controlled. Cheques should be written out by authorised personnel in designated and secure GoM offices.

There is also a lack of budgetary accountability by Principal Secretaries. The accountable Ministry raises each payment. However it is our understanding, though disputed, that the Accountant General makes the decision on which budget expenditure is allocated; this does not require the approval of the necessary controlling officer. We noted situations where expenditure allocated to one Ministry budget may not have been incurred by that Ministry.

Where a dispatch list is generated through IFMIS by the Ministry making payment, we noted evidence of additional payment vouchers being added to the dispatch lists after they had been generated and then being applied to the Ministry budget. Whilst we understand the need for effective cash management, each Minister and Controlling Officer is accountable for their budget and should be made aware of, and approve, any additions made. We recommend the provision of basic monthly and annual actual to budget positions to the relevant Minister and Controlling Officer. Consideration should also be given to providing clear procedures for standard financial management reports for each Ministry thereby allowing for transparency and facilitating comparisons being made between actual and budgeted spend.

We noted that no bank statements are provided to the accounting officers at each Ministry to allow them to reconcile their own transactions. This should be implemented with immediate effect; discrepancies should be flagged by the accounting officers to the Auditor General's Department.

Manual cheques were prepared for the period that IFMIS was closed following 'Cashgate'. We have not undertaken any work on the manual cheques but suggest that comprehensive audit work should be undertaken to ensure compliance, validity of payment and to check for any evidence of abuse.

In January 2013 the style of RBM cheque changed. Despite repeated requests we were unable to verify if any reconciliation was undertaken, confirm the location of the old style cheque books or if unused cheques were destroyed or cancelled. No evidence has been provided to support their destruction or to determine if they have been cashed. We therefore believe that further work is required by the NAO to confirm that these cheques have not been abused. We also recommend that the cheque sequences should be cancelled with immediate effect.

Neither the NAO nor the GoM Ministries we visited maintained a schedule of business ownership showing which businesses or political parties (where relevant) the principal secretaries and senior management figures owned or were members of. This would have aided the identification of any related party transactions and potential conflicts of interest. These records should be maintained going forward and annual updates should, be required. Importantly, during our work no conflict of interest registers were located.

The Auditor General undertakes financial audits of the government consolidated account. We have not seen evidence of any independent financial audits on the financial statements prepared by the various Ministries. Limited independent assurance can therefore be provided on government spend by Ministry. We understand that resources have now been redirected to undertake this task as a matter of urgency.

A cross check between the RBM list of bank accounts and the list provided by the Accountant General's Department was noted to be out of date suggesting that they were not aware of the number and types of accounts for which they were responsible.

There is unsatisfactory record keeping and filing of official documents making it difficult to trace records and vouchers. Basic filing techniques are not applied thus clouding the audit trail and leading to increased time being spent in tracing documentation. A lack of audit trail also increases the opportunity for concealment or fraud, theft or error.

There is currently a high level of use of gmail and yahoo accounts. This could result in information loss or breaches of confidentiality. Gmail and Yahoo accounts cannot be easily traced in government systems. We understand, however, that IFMIS has an internal mail capability and we recommend that the use of personal emails for official purposes is barred at the earliest opportunity.

Each individual Ministry maintains its own supplier list based on the database for its Ministry held in IFMIS. This makes the provision of spend data across suppliers time-consuming to obtain. Identification of things such as duplicate payments, favouring particular suppliers and general data quality is not therefore easy to achieve. Thus the benefits of oversight and cost efficiency through consolidated supply are not realised.

2.3. Outdated IFMIS software (EPICOR) operational environment

IFMIS is an integrated financial management system designed to reduce duplicate data entry; implementation of internal controls for transactions, reporting and information entry and the standardization of data classifications for financial events. IFMIS can integrate accounting-related information for larger organizational data management systems. It is used by government and private organizations.

Our review did not specifically cover the IFMIS environment as a later IT security audit will consider IFMIS in more detail.

Financial management systems are not new, they operate effectively globally on a daily basis. IFMIS data will only be as good as the data input into the system and the application of the security controls around it.

The deletion of any accounting entries and any subsequent payment of government funds is not a fault within IFMIS. It stems, instead from weak application of the controls by the individual users and by staff circumventing the controls designed to ensure that the system works effectively e.g. sharing user IDs.

We are unable to confirm if the individuals assigned to the user IDs that were implicated in the deletion of transactions are the actual individuals who removed the data lines or if their user IDs were compromised by others. This is because passwords are commonly shared or obtained by other means. We were informed that the IT administrator provided system administrator rights to the people identified as deleting records. We understand that these individuals have since been charged.

The IFMIS server is located in an unsuitable environment; it does not have adequate cooling or electricity back up facilities. During an inspection of the Government Wide Area Network (GWAN) server room it was noted that the temperature of the room was excessively hot. This indicates inappropriate temperature control and inadequate ventilation. There is no procedure in place to monitor the GWAN server room's temperature. The room has three air conditioners; however the operating efficiency of these air conditioners is not monitored. Overheating can lead to irrevocable damage to data IT network and information held therein.

Inspection of the network indicated a lack of Universal Power Supply (UPS) devices to ensure a continuous power supply to the network servers. Power outages and surges to the network may cause possible hardware failure, data loss and data corruption. Servers should be connected to a UPS device with adequate battery capacity to ensure uninterrupted power supply to the servers in the event of a power outage. This has hampered our work on IFMIS data extraction with constant power outages and rebooting. Such issues can also lead to IFMIS data corruption.

In addition during an inspection of the GWAN server room it was noted that the widows were left open after hours. This poses a security risk to the physical equipment as well as the information stored on the server's databases. The server room should be appropriately secured at all entry points.

During an inspection of the GWAN server room it was noted that the network cabling was disorganised and congested to the point at which network cable connection points could not be easily identified. This may result in lengthy details in solving network related problems. Network cables should be neatly organised and labelled to facilitate easy access traceability, of network connection points and prompt response to network trouble shooting.

Substantive testing in Ministries identified regular miscoding. For example we noted a payment voucher in the Ministry of Water Development and Irrigation for a subsistence allowance coded against a construction company. All payment vouchers should be correctly coded against the relevant supplier by the person responsible for data input. Individual supplier accounts should be allocated to managers whose are then responsible for reviewing and monitoring the expenditure posted to these accounts. Any discrepancies should be followed up.

We noted that 259 of the 598 records deleted were actioned outside of office hours (between 22:00 and 07:00 hours). The remainder took place during office hours. No exception reports are run or reviewed where these incidents could have been identified. Reviewing such exception reports on a regular basis would have helped the Accountant General's Department to identify potentially fraudulent or dishonest activity at a much earlier stage.

We have undertaken two attempted penetration tests of the IFMIS system using the IP addresses provided. To date we have been unable to access the system however testing will continue.

It was noted that there is no procedure in place to terminate the user profiles of departed employees and employees transferring from one Ministry to another. This may lead to unauthorised access to the Epicor system as well as unauthorised access to a particular Ministry's data. We recommend that user profiles should be terminated promptly for departing employees.

The bank statements' closing balances for account number 13006160078 were recalculated for August, September and October 2013 and we noted that the closing balances on the August 2013 and October 2013 electronic bank statements we were provided with appeared to be misstated by a total value of MK 1,120,572,678.35. Periodic checks should therefore be performed to ensure the completeness of banking transactions and subsequent action should be taken to understand, and react to, the cause of any discrepancies.

Transactions were deleted from the EPICOR system by users with system administrator access profiles. Fraudulent transactions may have been processed due to segregation of duty conflicts within a user's access profile. A user's access profile should be set up without segregation of duty conflicts. Segregation of duties is a key control process with the objective of preventing fraud and errors. Users' access profiles should therefore be assessed prior to access being approved and implemented by an authorised individual with the necessary knowledge of the EPICOR system.

Transactions were also deleted from the EPICOR system by users with access to the databases in which the transactions are stored. Users had system administrator access to the databases as well as to the entire EPICOR system which allowed them to process any transaction. Access to the databases should be restricted to database administrators only.

The EPICOR system does not facilitate the generation of supplier master file changes reports from a front end menu. Review of these reports would have indicated changes, and therefore potentially unauthorised amendments to supplier details. The regular generation of a supplier master file "changes" report should be implemented to facilitate the review and detection of unauthorised, in accurate and / or fraudulent changes.

2.4. Role of the Reserve Bank of Malawi

The GoM holds at least 554 bank accounts in Malawi Kwacha currency with the RBM, with the main GoM account being the MG1 Account. This account receives funding from the Malawian Revenue Authority as well as from international donors and subsequently transfers these funds to various accounts including the Development, Recurrent, Statutory, Deposit and Advance Accounts. The funds in these five accounts are used to pay the recurrent and capital development expenditure for the various Ministries, Departments and bodies of the GoM. The RBM allowed the audit team to supervise the extraction of electronic data for 11 bank accounts of interest (including those mentioned above) and provided access to the bank balances, cheques scans, files of cheque signatories and other supporting documents including foreign currency accounts.

The RBM operates under Law Chapter 44:02, one of its principal objectives being Part III 4 (b) '*to act as banker and advisor to Government*', the 'advisor' element suggesting active not passive involvement in managing client funds' availability. The RBM has informed the audit team it has no involvement in the qualification of payments and all cheques printed in the system are honoured regardless of available funds.

A supervised extraction of the RBM account data for the period 1 July 2012 to 30 September 2013 has been undertaken to gain some assurance that the full dataset had been provided. A database combining all electronic bank information has been created to identify inter account transfers and map fund flows. The database for the 11 bank accounts for the 15 month period contains 368,526 transactions.

The RBM has a memorandum of understanding (MoU) with GoM which states at 10.1.2 (2) states that '*the Bank in collaboration with Government shall ensure no fraudulent cheques are cleared in the system'*. We have particular concerns that high value cheques, including those with exact values on consecutive cheque numbers, were withdrawn on the same day. No evidence has been provided to show that these payments were, at any stage, challenged. We believe that these high value transactions could have been stopped were they subjected to more robust secondary checks.

2.5. Role of Commercial Banks' Operations

Our sample of 352 transactions identified 126 suppliers, organisations and individuals holding bank accounts with 19 banks including 11 Malawi based banks. We submitted the following information request to the banks:

- The bank statements for the period 1 January 2013 to 30 September 2013 for the relevant organisation;
- Information showing when the bank account was opened, by whom and a list of the signatories on the account(s);
- Details of any other bank accounts held by these companies and the directors/owners of said companies;
- Bank statements for any other accounts that these companies held with your bank for the period 1 January 2013 to date; and
- Any Suspicious Activity Reports (SARS) you completed and submitted to either, the Police, ACB or FIU in relation to these companies.

These requests for information were initially refused by seven Malawi banks citing client confidentiality. A formal subpoena was then issued by the Auditor General to the seven banks. Five banks complied with the subpoena. One required a Court Order that was duly provided and information provided without delay.

We have received good cooperation from the majority of Malawi commercial banks although requests for information are on-going.

No work has been undertaken in obtaining or accessing information from the international banks. Further work will therefore be required in this area.

2.6. Ministry Failings

All individuals receiving a payment from the GoM should be listed as suppliers on IFMIS. Consideration should also be given to including staff and government employees on IFMIS, especially where regular allowances are paid. This will make it easier to profile and to identify values paid.

ODPP should be able review the list of suppliers on IFMIS on a quarterly basis, raise concerns and send these concerns to the NAO.

We noted inadequate supporting documentation in the majority of cases with poor filing of payment vouchers. These should be filed, ideally in batch order, to improve audit trails.

We also noted that some of the internal audit functions within the Ministries focus on payment check processes rather than actually carrying out system and control reviews. Where internal audit acted as a 'prepayment check' function we have used their documents to support the validity of transactions.

Controlling Officers, Accountants and, potentially, Ministers should be provided with weekly, if not daily balances, on the MG1 and main sub accounts.

We further noted that authorisation levels are not determined based on monetary values. Goods and services can be procured as long as it is within budget and authorised as per the requirements of the internal purchase requisition. In our opinion controls should always reference monetary values as part of the authorisation process.

Payment Vouchers (PV) are created based on valid goods received notes (GRN), local purchase orders (LPO) and quotations. GRNs were missing to support a number of the PVs selected for detailed review.

During the walk through test we requested selected voucher lists. These could not be produced due the ineffective filing systems that are being maintained. As a result we were unable to trace our sample through a walkthrough of the controls and process.

Cheque payments are prepared at the central payment office based on voucher lists along with supporting documents provided by the cash office of the Ministry. During our review it was noted that there no reconciliations are performed between voucher lists and dispatch lists. All dispatch lists and voucher lists should be reconciled and the review thereof should be evidenced.

We noted that the financial statements in a number of Ministries that we visited were not independently reviewed or audited by the Auditor General. Financial statements should be independently audited by the Auditor General every financial year.

2.7. Office of Public Procurement

The audit team visited the Office of Public Procurement with the Auditor General and was introduced to the Director. A letter requesting various documents including the list of suppliers approved to provide goods, services and works to the GoM was issued and to date we have received good cooperation with the requested information having been provided. These details were checked for each of the sample selected.

3. Findings: Deleted Transactions

3.1. Background

Soft-Tech were requested by the Accountant General's Department in the Ministry of Finance to analyse the IFMIS database for the period 1 July 2013 to 30 September 2013 and determine if any transactions had been deleted and if so determine the extent of the deleted information.

In November 2013 Soft-Tech prepared a report identifying that 144 voucher journals and 133 payment journals totalling MK 5,656,134,300 and MK 8,682,916,313 were deleted following circumvention of the network firewall and system security.

The database of deleted transactions provided by Soft-Tech contains 598 lines of data. In some instances up to five lines of data (all the debit and credit accounting entries for a single transaction) have been removed thereby deleting the transaction in its entirety.

Soft-Tech provided the audit team with their report and supporting appendices which was reviewed and compared against other third party data sources to gain an understanding of each transaction.

It should be noted that the Soft-Tech report necessarily focuses on the accounting entry such as voucher, payment and journal entries. Our report focuses on the cash trail relating to those transactions.

The Soft-Tech report and supporting appendices has been used as the basis for the audit work completed on the deleted transactions and as such reliance has been placed on the accuracy of this report.

The deleted transactions are widely reported in the media and linked to 'Cashgate'.

3.2. Findings

Soft-Tech provided an appendix containing 598 lines of data on the deleted transactions. These 598 lines of data contain lines that relate to the same transaction and can be grouped to give 151 unique transactions. A comparison of these lines or data and transactions against the bank statements show that not all the deleted transactions were paid.

It should be noted that Soft-Tech have used the accounting entry figure in their report however we report on the actual cash payment that has been made through the banking system.

An analysis of the deleted transaction data was competed to identify the extent of the deletions and any trends or patterns.

The database analysis identified 144 voucher journals and 133 payment voucher totalling MK 5,656,134,300 and MK 8,682,916,313 were deleted from four different Ministries using different user ID, these being

- Irrigation and Water Development deleted using one user ID;
- Office of the President and Cabinet deleted using one user ID;
- Local Government deleted using two user IDs; and
- Rural Development and Tourism, Culture and Wildlife deleted using two user IDs.

One user name appears against deleted transactions for three Ministries.

The deleted voucher records were posted against one of five expenditure lines these being; construction of irrigation schemes; consultancy, contracts, maintenance of buildings and rehabilitation of roads and bridges.

The 598 lines of data containing 110 transactions have been paid from the Malawi Government Development account. This is the only GoM bank account found to date from which the deleted transactions have been paid.

The highest value deleted transaction was MK 408,768,000 and the lowest was MK 231,339.

The highest value deleted transaction that was not paid was MK 396,458,744 and the lowest was MK 228,675. These cheques may have been printed but not presented at the bank for payment and should be cancelled.

The cheques for deleted transactions for Tourism, Wildlife and Culture and the Office of the President and Cabinet were all sequentially numbered and all were honoured for payment suggesting that a premeditated decision was made to use certain batches of cheques. In contrast the cheques relating to deleted transactions for Irrigation & Water Development, whilst also sequentially numbered, have not yet been traced to a bank, this would suggest they have not been paid.

A similar pattern has been noted with transactions allocated against the Local Government and Rural Development, wherein we have noted sequentially numbered transactions with some traced and identified as paid and other not traced as payments from the bank.

At present all deleted transactions are noted to be paid from the Malawi Government Development Account.

A review of the 598 lines of data identified the following;

- The deleted transactions for Irrigation and Water Development contain 20 high value transactions that were deleted but not paid suggesting that the cheques were issued but never presented for payment and that the intended beneficiaries may still have the cheques in their possession. The five highest value transactions allocated against this Ministry but not paid were MK 168,420,000, MK 165,796,000 and MK 165,784,000; MK 91,320,000 and MK 75,320,000. The cheque stub deletion dates for all these transactions is 9 September 2013 suggesting that the individuals who were originally given the cheques were then told not to present them for payment;
- Some of the paid deletions transactions contain only the vouchers journals, some just payment journals and some contain the voucher journals, payment journals and the voucher journals for the withholding tax entry (being all the lines relating to that transaction);
- Analysis of the deleted transactions shows that blocks of data with both high and low value transactions were deleted suggesting that the low value transactions may be genuine payments and have been accidentally deleted due to their proximity to the high value transactions (i.e. cheques 017339 to 017348 allocated to Tourism, Wildlife & Culture were deleted on 5 September 2013 and contained transactions ranging from MK 310,000 to MK 396,023,569).

We noted transactions identified as deleted in 2011 per the Soft Tech report. We tested a small sample of these transactions to determine if payment had been credited to the bank account of the relevant company. No payment could be traced, however we believe the sample size should be increased.

3.3. Summary

The username IDs of four individuals have been used to delete detailed financial information from the GoM financial management system, IFMIS.

Not all the deleted transactions have been cashed at the bank. Batches of sequentially numbered cheques have been allocated against various ministries suggesting premeditated and organised action.

A range of cheques were issued in sequence by the Ministry for Tourism, Wildlife and Culture and the Office of the President and Cabinet. This again suggests premeditated action.

Cheques have been raised through IFMIS, potentially printed but not cashed at the bank. These cheques should be cancelled forthwith.

Lines of data relating to transactions have been deleted outside of normal business working hours.

Not all of the transactions that have been deleted have been paid.

We noted that none of the deleted transactions that related to the Ministry for Irrigation and Water Development could be traced to the bank statements. This would suggest that they were not paid and the funds were not lost/stolen.

We have noted questionable transactions in the bank statements of companies on the deleted transaction database without supporting paperwork that was not deleted from the IFMIS system. This would suggest that there are other payments made that were not deleted from IFMIS.

We noted additional transactions considered to be fraudulent that were not deleted from the IFMIS system.

3.4. Payments Made To Companies

We reviewed the payments identified on the deleted transaction list to confirm that they have been paid through the recipient's bank and how those payments were then utilised.

We noted the following anomalies:

- Companies that were typically registered as building and engineering companies and had been established for at least five years. In most instances, the companies have no internet presence, supporting documents would suggest turnover was low with bank activity limited as such they are unlikely to be of a sufficient size or have a historical track record that would enable them to secure the high value government contracts which the funding they received appears to indicate.

- Companies receiving funds allocated for consulting activities were operating with recent or previously dormant bank accounts with limited banking activity prior to the government payment.

- Payments were made to the recipient company in the form of cheque payments from the GoM Development Account Number 13006160082.

- Prior to receipt of the government payment, the company accounts often showed limited evidence of business trading or we noted that they were trading on a comparatively small scale that resulted in the payment in to the account appearing as an unusually large payment.

- In most instances, account balances were either zero or overdrawn prior to the deposit.

- Once the government cheque had cleared the business account we noted that withdrawals commenced with immediate effect, suggesting that GoM cheques are guaranteed and can be instantly drawn down. In the majority of cases withdrawals are in cash or to a lesser extent, transfers to other, as yet unknown accounts or forex transactions. Cash transactions ranged from ATM withdrawals, typically up to account limits of MK 40,000 to cash withdrawals at the bank exceeding MK 100,000,000. All of this implies fraudulent activity.

- The bank statements of one company show that an amount of MK 516,500,000 was withdrawn in cash or encashed cheques in one day and a further MK 550,000,000 was withdrawn by similar means by the same company from the same bank two days later. This is one of a number of examples of large scale cash withdrawals from a commercial bank. Further work is required to establish the whereabouts of these and other similar cash deposits.

- The deposited government funds would typically be withdrawn in full over the following three weeks.

- We have established that certain individuals, who are employed by Ministries or involved in government, have been linked to two or more of these companies. This link has been established by identifying that the owner of one company has been identified as also being a signatory to another business account and has been identified as making withdrawals from these other business accounts. We have also established that government employees have owned or at least been signatories to one or more accounts and have made withdrawals against these government deposits.

- Ministries have been unable to provide supporting documentation, such as invoices, contracts, GRNs or any other evidence of any service or goods being provided to justify the payment made from the government account.

- In the majority of cases the business owners who have received these deposits stated that they had not bid for government work or provided any services that would prompt payment into their business accounts.

- We noted transactions where the payments made could be classified as genuine, being supported by adequate third party documentation such as court orders for outstanding debts. Refer to table below:

3.5. Identified Amounts

The amounts below are the 'Cashgate' related amounts identified to date:

No.	Company	Ministry	Amount MK	Amount %
1	Company 1	OPC / Tourism, Wildlife & Culture	1,860,584,273	30.5%
2	Company 2	OPC / Tourism, Wildlife & Culture	1,140,738,289	18.7%
3	Company 3	Tourism, Wildlife & Culture / Not known at present	793,716,802	13.0%
4	Company 4	Tourism, Wildlife & Culture	516,764,229	8.5%
5	Company 5	Tourism, Wildlife & Culture	401,088,916	6.6%
6	Company 6	OPC / Local Government & Rural Development / Not known at present	237,459,967	3.9%
7	Company 7	Tourism, Wildlife & Culture	265,340,865	4.4%
8	Company 8	OPC / Tourism, Wildlife & Culture	173,613,572	2.8%
9	Company 9	OPC / Tourism, Wildlife & Culture	131,224,494	2.2%
10	Company 10	Tourism, Wildlife & Culture	131,224,494	2.2%
11	Company 11	OPC / Tourism, Wildlife & Culture	123,865,679	2.0%
12	Company 12	Tourism, Wildlife & Culture	117,530,501	1.9%
13	Company 13	Tourism, Wildlife & Culture	84,963,341	1.4%
14	Company 14	Tourism, Wildlife & Culture	63,542,083	1.0%
15	Company 15	Tourism, Wildlife & Culture	30,654,079	0.5%
16	Company 16	Tourism, Wildlife & Culture	24,179,121	0.4%
	Note: OPC is the Office of President & Cabinet		6,096,490,705	100.0%

These amounts have also been arranged by ministry below:

No.	Ministry	Amount MK	Amount %
1	Tourism, Wildlife & Culture	3,736,791,727	61%
2	Office of the President & Cabinet	2,126,654,976	35%
3	Local Government & Rural Development	151,635,967	2%
4	Not known at present	81,408,035	1%
		6,096,490,705	100%

Transactions allocated against Irrigation and Water Development were deleted but not paid and as such do not appear in the above tables as these focus on following the cash trail.

3.6. Examples

The sensitivity of our findings and the potential legal action limits our opportunity to report in detail without prejudicing potential future legal action. The examples given below provide a summary of two types of cases where failures have led to the loss and theft of Government funds to demonstrate the nature of our findings.

Information relating to our work on the following cases will be referred to the Malawi Law Enforcement Agencies (being the ACB, Police or Financial Intelligence Unit) through the Auditor General. As such we have restricted the level of information provided in this report.

Example Deleted Transaction Payment - Company A

Company A was registered in July 2005. The report by Soft Tech identified 12 voucher journals and nine payment journals in the period 1 July to 30 September 2013 in relation to this company that had been deleted from IFMIS.

A review of the Government of Malawi bank statements identified six transactions totalling MK 1,860,584,273 that matched these voucher and payment journals and were paid from the Malawi Government Development account into Company A's commercial bank account.

No documentary records, including payment vouchers, invoices, receipts or procurement files to support these six transactions, could be traced and no evidence of the supply of goods, services or works to support the payments made to Company A could be provided.

Emails requesting documents to support these transactions was sent to the Ministries against which the payments had been allocated, these being the Ministry of Wildlife, Tourism and Culture and the Office of the President and Cabinet (OPC). Emails were also sent to the Accountant General's Department and ACB.

ACB were the only organisation to respond and confirmed they did not have these documents and were also trying to locate them. The Ministry of Tourism, Wildlife and Culture, the OPC and the Accountant General did not respond to the request.

The process for recording cheque payments requires that all cheque payments should be recorded on the Dispatch List. The Dispatch Lists for the period 1 April 2013 to 30 September 2013 were reviewed but no evidence of the cheque payments to Company A could be found.

A review of the bank statements for Company A shows that the six payments from Government were banked in two separate amounts.

A total of MK 603,541,256 was paid in on 20 August 2013 taking the bank account balance to MK 486,994,844. Over the next eight days MK 489,517,120 was paid out in cash, cheques, transfers and via email requests. On the 28 August 2013 the account was overdrawn by MK 2,522,276.

On the 28 August 2013 five further amounts totalling MK 1,737,043,017 including a transfer from an overseas company were paid into this account increasing the balance to MK 1,734,520,741. Over the next eight days MK 2,121,286,287 was withdrawn in cash, cheques and by email requests on the 5 September 2013 the account was overdrawn by MK 336,690,280.

On the 6 September 2013 a transfer of MK 250,000,000 was made from a related company (Company B) also under review as part of the 'Cashgate' investigation and our review. This payment was made into Company A's bank account reducing the bank balance to MK 86,690,280 overdrawn. The transfer of MK 250,000,000 was funded through transactions which were also deleted from IFMIS and link to 'Cashgate'.

An examination of Company A's bank statements shows that, in the four day period from 2 to 5 September 2013, a total of MK 1,265,150,000 was withdrawn in cash or as encashed cheques with MK 516,500,000 withdrawn on 3 September 2012 and MK 550,000,000 withdrawn on 5 September 2013. Based on the 'Currency in Circulation' figures provided by the RBM these withdrawals were equivalent to over 1.4% of the Malawian Kwacha in circulation at the time.

The commercial bank filed a Suspicious Transaction Report with FIU in relation to Company A's financial activity on 29 July 2013 in regards to other transactions that preceded those discussed above. These transactions are under review as part of the corruption element of the report.

In summary no tangible goods, services or works appear to have provided to support the MK 1,860,584,273 paid to Company A. On the basis of the evidence provided to date the possible offences of theft, fraud, money laundering and conspiracy to defraud Government should be considered.

The cases completed to date have been or will be in due course referred to the ACB for further action.

3.7. Example Deleted Transaction Payment - Company B

Company B was registered in May 2013 at the Registrar of Names in Blantyre noted to trade as 'General Trading'. In June 2013 it opened a bank account in City Centre Lilongwe.

The bank account commenced activity in June 2013. Account transactions ceased on 30 September 2013 leaving the account with a credit balance of MK 150,157,853.88.

On 22 August 2013 Company B received two payments totalling MK 516,764,228.54 from the Malawi Government Development a/c 13006160082 for MK 349,568,230.96 and MK 167,195,997.58 respectively. No records relating to the transaction have been traced. No records, such as payment vouchers and invoices relating to the transaction, have been traced. At the time of this report it is unclear what these payments relate to.

Transactions valued at MK 1,323,094,738.37 were debited from the account and MK 1,473,252,592.25 credited to the account. However five transactions with a total value of MK 950,000,000 net each other with matching debits (noted as repayment of principle) and credit values (noted as fixed deposits). This would suggest that payments were made into the account to mask the true activity on the account.

A sample of 13 cheque images obtained from the bank show 12 bearer cheques to a value of MK 194,630,000 made to 'cash' with the signature consistent of that held as a specimen for the owner.

Conclusions

Company B was registered in May 2013. We believe it was formed for the sole purpose of laundering government funds.

Various funds movements take place to mask the actual activity of the account.

No procurement details have been provided, no 'no-objection' relating to any procurement has been registered or noted with ODPP.

No other supporting documents have been traced to confirm the purpose of the payments.

We understand that the account balance of MK 150,157,853.88 has been frozen by ACB. The charges of theft and money laundering should be considered.

At this stage it is not clear where the MK 950,000,000 that flowed through the account originated.

3.8. Example Funding Misuse - Transactions to Company C & D

We have been provided with documents relating to the supply of Produce A by Company C and Company D; both companies are claimed to be international companies.

Company C

Company C is the chosen supplier of Product A to Ministry A. No procurement documents were provided to support their selection despite numerous requests. We were informed that suitable due diligence had been undertaken on the company though this could not be provided because the Ministry A had worked with Company C for '*a number of years'*. At a later meeting this was revised to Ministry A suggesting to us that 'it *did not identify the two companies to supply the goods in issue and that the same was done by government.*' No evidence to support this claim can be provided.

Our research suggests that Company C was registered on 1 April 2012. The address is noted to be the same as the company secretary suggesting the address is a registered office and accommodation address. Company C is linked to a number of other companies although the details suggest that the company has no financial standing and is not a supplier of Product A. The selection of Company C by the Ministry A is questionable.

Company D is also noted in related transactions and connected documents with Ministry A, Company C and Product A. Certain documents would purport to be signed by an individual linking Company C and B.

Company D

Payments are noted to be made to Company D for Product A. The address of Company D can be traced to that of a different business selling Casual Wear; Denim Garments; Jeans and Sport Suits. We do not believe the two companies linked to that address are related.

We were informed by Ministry A that Company C stated that '*under its national law it would not be permissible to supply the goods of the quantity contracted for under a single contract'* Ministry A states that it '*followed the recommendation of Company C to split the consignment into Company C and D'.* This would suggest that Company C were unable to fulfil the required contracted supply.

We can find no registration details for Company D in its chosen country of operation. No ownership details can be found.

No supporting documentation to support the due diligence or selection of Company D have been provided by Ministry A.

Company D has no financial standing or history and is not a supplier of Product A. The selection of Company D by Ministry A would seem, at best, questionable.

It is unclear to us why the Ministry chose to support a new supplier in contravention of another government's national law.

In our opinion the company may be fictitious and all payments could therefore be considered as fraudulent unless evidence can be proven otherwise.

Trading with Company C and D

We have been able to trace eight payment transactions between GoM and Company C and B between September 2012 and August 2013.

In total MK 5,392169,563.40 was paid to Company A in five transactions from Ministry A and Malawi Government ORT accounts. Company B received MK 4,542,236,482.99 between the July and August 2013.

We were informed by Ministry A that both companies had been regular supplier to Government and Ministry A. We found no evidence of any previous trading activity with these companies. We were later informed that these suppliers had been recommended as approved suppliers to other government department, despite agreements supporting evidence would be provided, this has not happened.

The Malawi Revenue Authority has confirmed that they have no records of imports relating to customs declarations for Company D.

It should be noted that Ministry A would only supply 'photocopy' copies of all documentation relating to companies C and D. Ministry A commented that '*all original offer letters are issued to the supplier and it only retains copies'* We find it unusual that at least one copy of the offer letter would not be signed and retained on file.

There are regular inconsistencies in the documents provided by the Ministry A. On the 8 June 2012 Company C issued a pro-forma invoice (no 083/12) to Ministry A in relation to Product A at a list price of USD $5,490. On the 26 June 2012 a further pro-forma invoice (104/12) is issued for 3,000 Product A with a total value of USD $ 16,470,000. Terms are 40% advance followed by 15 equal monthly payments. Such terms could only be agreed by the Minister as per the Public Finance Management Act (No 7 of 2003) Part VII Borrowing, loans and guarantees. No evidence of this agreement can be traced.

On the 29 June 2012 Company D issued two pro-forma invoices both referenced Ministry A 1002 for 3,300 and 3,900 Product B (a similar but lower specification version of Product A) respectively with an item price of USD $5,438 Product (USD $58 cheaper than the Company C quote).

On the 10 July 2012 a local purchase order and letter of contract award was issued to Company C for 1000 Product A at a quoted price of USD $5,490,000.

A letter requesting ministerial approval is dated 15 August 2012 and suggests use of MK1.5 billion funds from Treasury. Reference is also made to the purchase of an additional 6,900 of Product A with 3,300 from Company D.

On the 24 August 2012 local purchase order LO07 was issued for 6,900 of Product A in the name of Company C. On the same day two further awards of contracts were issued, one for 3,000 of Product A to Company C one for 3,900 of Product B to Company D.

Two 'local currency conversion forms for foreign currency' were issued in respect of payment to Company A for 'equipment for XXX' the payments are made from the Ministry A ORT account for $5,490,000 to two separate bank accounts for Company A.

No payments were noted to be paid to Company D in 2012.

No delivery notes or records of receipt of good provide by Company C have been provided in relation to these payments.

No record of the imports of Product A are recorded with the Malawi Revenue Authority Customs department until 14 November 2013.

No invoices, other than pro-form invoices, have been provided to support these payments. A pro-forma invoice is a document used by a seller as an 'intention to sell'. It is usually provided prior to dispatch of goods, i.e. in effect a confirmed purchase order. As such it is not a true invoice and should not be used for accounting purposes.

No contracts have been provided for any of these procurements.

In the absence of any evidence of delivery such as copies of the local purchase order, an invoice and goods received note attached to the payment voucher. The advance payment to Company C was not in accordance with Treasury Instructions 'Payment Procedures to Suppliers'.

On the 17 July 2013 Company D issued a pro-forma invoice for 4,000 of Product C (being a spares kit for Product A) at a price of USD $485 per unit with a total contract value USD 1,940,000. A letter of award is issued on 22 July 2013 on the 8 August 2013 a payment for MK 665,174,396 is made to

Company D from the Malawi Government ORT account FTC Reference 001FTC1132200018. No financial transfer documents were provided to support this transaction however we believe this relates to this procurement. A delivery note suggests that a delivery of 25 cartons was received in August 2013. This was supported by Malawi Revenue Authority importation documents on the 21 August 2013 for Product C valued at MK 670,481,859.00.

On 25 July 2013 a payment for MK 1,997,861,671.59 was paid from the Malawi Government ORT account with foreign currency transaction reference FTC 001FTC1132060001 to Company D.

There was no evidence of delivery, such as a copy of the local purchase order, an invoice and goods received note attached to the payment voucher. The advance payment to Company D is contra to Treasury Instructions 'Payment Procedures to Suppliers'.

No suitable or original evidence has been provided to support the payment being made for goods or services rendered. As such MK 1,997,861,671.59 should be classified as theft of Government Funds and subject to recovery action.

On the 12 August 2013 Company B issued invoice number 5545 in relation to 1,000 of Product A with an invoice value of USD $5,438,000. On the 21 August 2013 a payment for USD $5,438,000 (MK1, 879,200,415.40) was paid from the Ministry of Defence ORT account under foreign currency transaction reference 001FTC1132330020. Supporting government documentation makes reference to 'anti-riot suits and protective equipment for Ministry A. No reference is made to the Product A.

No further documentary support has been provided.

It is noted that two shipments of Product A arrived at KIA airport on the 14 and 27 November 2013 consecutively. As per customs documentation the shipments were valued at MK 4,501,067,403 and MK 4,658,550,796 respectively.

On the 15 November 2013 Company D issued a delivery noted for 1000 Product A, on the 27 November 2013 Company C issue a similar delivery note for 1,000 Product A. We believe these delivery notes may be related to the imports noted above.

On the 30 October 2012 MK 977,669,503.02 was paid to Company C out of the Malawi Government ORT account under foreign currency transaction reference 001FTC1123040005. No evidence to support the payment or the goods can be traced.

On the 22 November 2012 MK 979,834,892.40 was paid to Company C out of the Malawi Government ORT account under foreign currency transaction reference 001FTC1123270012. No evidence to support the payment, or the goods themselves, can be traced.

In the absence of suitable or original evidence being provided to support the payment for the goods or services rendered, MK 1,957,504,395.60 should be classified as theft of Government Funds and subject to recovery action.

Product A Purchases Value For Money

The recommended price of Product B is USD $727 (USD $950 per US industry recognised valuation book). No listing appears for Product A. However contact with retail suppliers (not wholesale) would suggest that the maximum price for Product A, purchased by Ministry A allowing for additional extras would be nearer to USD $1,500 per item.

Information obtained from Ministry A identified requirements for similar products to Product A. This included a widely known US equivalent item, the cost price per the requirement sheet being USD $300 (reflective of researched prices). Interestingly the main supplier would be that of an industry known manufacturer and supplier

We physically verified (without opening sealed cases) 100 wooded crates purporting to contain 10 Product A per case. The verification exercise was undertaken at Lilongwe Airport. The cases had no distinguishing marks however were stamped with consistent information.

Customs declaration/Asycuda documents relate to two consignments suggest both consignments are noted to be exported by Company C, imported by Ministry A using a shipping company.

In the absence of any competitive international tender and linked to the restrictive single source tendering we believe these purchases to be in excess of their true cost by a minimum of USD $ 3,938[1] per Product (265%) resulting in a loss to the Malawi Government of USD $3,938,000[2] in relation to the January 2014 shipment alone.

Product B Magazine Spare kits Value for Money

On the 17 July 2013 Company D issued a pro-forma invoice for 4,000 of Product B spare kits at USD $485 per unit with a total contract value USD 1,940,000.

[1] Lowest price paid $5438 less estimated actual cost $1500 = $3,938.00

2 1000 items included in the January 2014 shipment (1000x$3938=$3,938,000)

Our work would suggest the maximum price for these kits is approximately USD $ 30. Even assuming that the purchased kit includes other spare parts the maximum price per kit would be approximately USD $ 150.

In the absence of any competitive international tender and linked to the restrictive single source tendering we believe these purchases to be in excess of their true cost by a minimum of USD $ 335 per kit (223%) resulting in a loss to the Malawi Government of USD $1,340,000.

Conclusions

Company C and B do not have trading history. Company C was formed two months prior to its selection as a key supplier to government. No legal registration of Company D can be traced.

GoM cannot provide any evidence of due diligence of either company to check their suitability as suppliers to the government.

Malawi Government funds have been provided in advance of need, without suitable monetary guarantees, unsupported by suitable paperwork and not in compliance with the agreed terms.

No evidence of the procurements can be found with the ODPP. Given that the procured items have to be declared to the United Nations and released publically, we would not expect them to be classified as security restricted for procurement purposes.

No competitive tender was undertaken.

The products should have been subject to international procurement to obtain best value. This did not happen.

The supplier chosen is not a known supplier of the procured products. It is not clear how they were introduced to Ministry A.

The supply volumes do not match those published by the relevant United Nations oversight body.

Limited original documentation can be provided by Ministry A to support the purchases.

No invoices have been provided with payments based on ‘pro-forma’ invoices.

We do not dispute that some items have been supplied. However the documentary evidence provided would suggest that these were significantly overpriced and not in the quantities contracted.

MK 5,979,039,979.20 has been paid into three different bank accounts on behalf of Companies C and D. Based on external price verification MK 3,619,539,979.20 has been stolen/mis-procured in relation to these procurements.

Additional payments totalling MK 3,955,366,067.19 have been made. At the time of this report no supporting evidence has been provided in relation to these payments. In the absence of suitable evidence consideration should be given to the arrest and the charge of theft of those involved in the approval of payments.

Consideration should be given to the recovery of lost government funding in line with Treasury Instruction.

The high value of these overpayments would suggest that neither Company C nor Company D are the ultimate beneficiaries of the funds received. Further work with International Law Enforcement Agencies should be undertaken.

Additional cases will continue to be subject to analysis and investigation until the close of our work.

These cases will be referred to the relevant Law Enforcement Agencies for further investigation.

Report ends.

APPENDIX 1

Recommendations

The recommendations listed below have not been discussed with the relevant Ministry or Department. They are necessarily based on our work and observations noted while interacting with the control environment.

The list is not deemed to be comprehensive and we understand work has already commenced to enhance the control environment, as such some of these recommendations may already have been implemented.

Ref	Recommendations
1	Further work should be undertaken to continue the investigation into the remaining cases.
2	Funding transfers to international jurisdictions should be traced until the final beneficiary accounts are identified.
3	A clear job description for the role of Accountant General should be prepared. This document should be used as an aid in defining the roles of all departments within the Ministry of Finance.
4	The Accountant Generals Department should set up an effective filing system that allows easy location of all documentation. This process should include effective archiving procedures.
5	A procedure manual should be prepared within the Ministry of Finance. Staff members responsible for the design and future updates should be clearly identified, with periodic reviews being undertaken.
6	The cheque approval process within the Accountant Generals Department should be reviewed and accountabilities implemented. All staff involved in the checking and approval of payments should be advised of their role in the process and provided with guidance where necessary. Any member of staff required to sign off on a cheque payment must confirm that all supporting documentation is complete and correct.
7	In compliance with TI 2.4.11 bank reconciliations should be completed for all accounts maintained by the RBM by the Accountant Generals Office. We would expect bank reconciliations be undertaken at least daily until they are on top of the reconciliations at which stage they can move to weekly.
8	Confirmation that bank reconciliations are taking place and that all un-reconciled figures are investigated promptly and effectively should be undertaken by internal audit on a periodic basis.

9	Preparation of cheques should be carried out in a secure environment only. Responsibility for enforcing this control should be clearly allocated within the Accountant Generals Department.
10	Budget responsibility must be accepted by each ministry. The Accountant Generals Department should, as part of their month end processes, issue monthly financial performance reports to each ministry. These reports should be detailed enough to allow responsible accountants within each ministry to confirm that all expenditure allocated to their cost centres is posted correctly. A mechanism should be implemented that allows ministries to report miss-posting resulting in miss-posted entries being re-allocated to the correct cost centre.
11	As part of the monthly finance performance reporting noted above, clear reference of actual expenditure against each budget should be made
12	The Accountant Generals Department should maintain a list of all government accounts with RBM. Any requirement to open new accounts should be subject to approval by the Accountant General.
13	A detailed manual for the use of IFMIS should be prepared by the Accountant Generals office. The manual should include all required IT controls such as avoiding sharing log in details. The manual should also address environmental factors.
14	An exercise between the Accountant Generals Department and the RBM should review the current list of at least 554 bank accounts held by the GoM. An assessment of the need for each account should be carried out and all dormant or unnecessary accounts should be closed with immediate effect. The exercise should provide a list or chart of all accounts in operation, including areas / ministries covered and a list of signatories. Any amendments to this list / chart should require authorisation by the Accountant General.
15	Effective reporting of expenditure against budget should be provided to Controlling Officers, accountants and Ministers where required.
16	Authorisation levels, once defined should be set up in Epicor.
17	Regular testing of the IFMIS data should be undertaken including exception reports until such time as confidence can be regained in the accuracy of the inputs and data set.
18	The practice of adding additional payments to IFMIS dispatch lists should cease with immediate effect.
19	All payment vouchers should be filed by batch or date order.

20	Cheques should be treated as secure documents (similar to cash) cheques batches should be held securely and regularly reconciled with evidence held for audit purposes. Outdated and old style cheques should be deleted immediately.
21	Access and exception logs for IFMIS should be reviewed at least monthly looking for unusual transactions and suspicious activity timings. The reports should be forwarded to the NAO and Internal Audit department
22	The capacity of the Financial Intelligence Unit should be increased to allow analysis of trends and pattern all in-depth assessment of high risk transactions.
23	The reporting lines of the FIU should be reconsidered to ensure cases investigated can be progressed.
24	FIU should be provided with read only access to the Reserve Bank systems to integrate on-going monitoring for suspicious transactions
25	FIU should have an overview of the commercial bank electronic payment system relating to international payments.
26	To reinforce the payment approval process, government should enforce TI 5.26.8 resulting in the authorising officer being personally liable and surcharged in respect of any incorrect payment
27	All payments for expenditure over MK 10,000,000 should be approved by the responsible Principle Secretary. Details should be provided to the Auditor Generals Department.
28	Consideration should be given to changes in the Reserve Bank MOU with Government to ensure adequate provisions are in place to limit the clearance of potential fraudulent transactions.
29	The ability of using IFMIS for e-mail should be investigated. Use of general internet accounts should not be allowed.
30	All individuals receiving payments, including allowances, from GoM should be recorded as supplier in IFMIS.
31	Authorisation levels within ministries should be determined. These should be based on monetary values. Any attempt to by-pass authorisation controls should be treated as a disciplinary offence.
32	Individual Civil Servants who receive payments in the form of allowances should be added to the IFMIS system to allow payments of allowances to be tracked and profiled.

33	The use of pro-forma invoice to support payments should be stopped with immediate effect. Where payment is made on a pro-forma invoice this should be approved in advance with the relevant Principle Secretary who all accept all responsibility relating to accuracy of the payment.
34	Where Government funds are provided in advance adequate security bonds should be provided by the supplier prior to the payment being made. Where Government Funds are provided without suitable security in place, the wording on the approval should be change to place liability for any funds loss on the approving officer.
35	Government should commence legal action, with immediate effect, to recover funds from those suppliers who have received advance funding but not supplied the contracted goods or services.
36	Controlling Officers, Accountants and potentially Ministers should be provided with weekly if not daily balances on the bank accounts they are responsible for. This should include the MG1 account and related sub accounts.
37	Controlling Officers, Accountants and potentially Ministers should be provided with budget versus actual reports for spend relating to their vote on a weekly/monthly basis.
38	Appropriate security cleared staff should be engaged. To undertake audits of the security sensitive ministries. All Government Ministries should be subjected to internal audits including MDF, Police and Ministry of Defence.
39	The duties of the Commercial Banks to issues STRs should be reiterated.
40	Consideration should be given to moving to electronic payment method for certain transaction.
41	The importance of IT security should be reiterated appropriate disciplinary action taken in relation to breaches.
42	A programme of whistleblowing for corruption activities should commence with sensitisation and support to those who raise concerns. This should be well publicised.
43	Comprehensive review of all Malawi company import export agency payments and contracts with Government to ensure suitable Value for Money is being obtained.
44	The Internal Audit Directorate should include a detailed review of the application of the Public Finance Manual and Treasury Instruction in their annual plan.

45	Internal Audit should ensure that an effective review of the application of the use of manual cheques during the shutdown of Epicor takes place. The review should consider compliance with manual processing procedures and should consider if any abuse of funds took place.
46	An IT internal audit schedule of key IT controls should be prepared and implemented. All findings should be followed up and shared with the Accountant General and the Auditor General
47	Accounting officers at each ministry should be provided with copies of relevant bank statements to allow independent review of each ministries accounts.
48	Reconciliations should be carried out between voucher lists and dispatch lists. Evidence of reconciliation should be recorded and any non-balancing items should be investigated immediately
49	No payment should be made without adequate supporting documentation including actual final invoice not pro-forma invoices.
50	Adequate due diligence procedures should be undertaken on all new suppliers (in particular for high value international supplies) with clear audit trail maintained.
51	A reconciliation of old format cheques should be undertaken against paid cheques. All unused and missing cheques should be cancelled and destroyed. If any unallocated cheques have been found to be cashed, then an investigation should be carried out with immediate effect.
52	The NAO or each ministry should maintain preferred supplier lists that are publically available. These lists should include details of ownership and any ownership by members of staff or political figures should be recorded.
53	The Auditor General should undertake independent financial audits of all ministries on an annual basis.
54	National Audit Office should undertake annual financial statements audits per Ministries for publication.
55	National Audit Office should undertake regular reviews of the GoM bank statements to limit the opportunity for funding misuse. These audits should include testing of RBM sample data.
56	ODPP should be provided with access to IFMIS supplier lists on a quarterly basis. Access should allow ODPP sufficient access to allow effective interrogation of supplier details. Results should be shared with the NAO on a quarterly basis.

57	ODPP should review the list of supplier from IFMIS for each Ministry on a quarterly basis; any concerns should be forwarded to the NAO. The review will allow government to improve purchasing through consolidated contracts and limit the opportunities for unapproved or non-contract supported companies to receive Government Funds.
58	The Reserve Bank should maintain adequate auditable files to show communication with government to support the approval of payments.
59	Due to the nature of the operation of a reserve bank, the RBM should ensure that it has the capabilities, in terms of staffing and access to software, for the various audit teams that will inevitably require data on an on-going basis. RBM should have designated 'read only' access for approved auditors and staff available for gathering required information.
60	In compliance with Chapter 44.02, the role of the RBM and its relationship with the Accountant Generals Department should be clearly defined. The relationship and MoU should be updated where appropriate. The MoU should clearly define the RBM in terms of managing funds availability, cheque signatories, particularly for large value payments and assessment of unexpected increases in cash demands by commercial banks. RBM should implement review processes that can provide assurance that all MoU responsibilities are being met on a periodic basis.
61	The RBM should maintain adequate auditable records to support communication with Government relating to approval of payments.
62	Efforts should be enhanced to locate the cash disbursed to companies included in the Cashgate scandal from company 1 to 16 accounts