

National Audit Office of Malawi

“Cashgate” A Summary Report on the Findings arising from work carried out into Fraud and Mismanagement of Malawi Government Finances

This report covers transactions and controls in the six month period 1 April 2013 - 30 September 2013

Report Issued 25th September 2014

Contents

Contents	2
Baker Tilly Risk Advisory Services LLP	3
1. Abbreviations	4
2. Introduction	5
3. Background.....	6
4. Scope of the Review	9
5. Summary of Findings.....	10
6. Limitations.....	18
7. Quantification of loss.....	20
8. Review of 'Cashgate' cheques	23
9. Review of 'procurement fraud' payments	24
10. Accounting Entries Deleted but Cheques Not Cashed	28
11. Payments to 'Cashgate' Businesses but Accounting Entry Not Deleted from IFMIS.....	29
12. GoM Cheque Signatories	30
13. Controlling Individuals.....	31
14. Links between businesses and parliamentary candidates.....	32
15. 'Cashgate' businesses.....	33
16. Cheque Sequencing	34
17. Cash withdrawals.....	35
18. Bank Accounts Opened Prior to Receiving 'Cashgate' Funds.....	37
19. Transfers between Cashgate businesses.....	38
20. Payments to legal practitioners in Malawi.....	39
21. Businesses registered in 2013.....	40
22. Withholding Tax.....	40
23. Cash Withdrawals In USD	40
24. Information Systems Review	41
25. Acknowledgement	43

Baker Tilly Risk Advisory Services LLP

Our report is provided for the use of the Auditor General of the Government of Malawi. The review by Baker Tilly Risk Advisory Services LLP funded by the UK Department for International Development (DFID), and the report is provided under the terms of the framework agreement between Baker Tilly Risk Advisory Services LLP and DFID and the specific contract for this review. This report is provided solely for the purpose of summary reporting on the case files handed over to the Auditor General in accordance with the terms of our engagement and for no other purpose. Our report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights against Baker Tilly for any purpose or in any context. Save for any responsibility to the addressees of this report, to the fullest extent permitted by UK law, we will not accept or assume responsibility or liability to anyone in respect of our services and we shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on, or representation in, this report. Our report shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent except to parties, including law enforcement agencies, demonstrating a statutory right to see it to whom we accept no responsibility.

A copy of this report has also been made available to DFID as the funders for this review.

© 2013 Baker Tilly Business Services Limited

Baker Tilly Tax and Advisory Services LLP, Baker Tilly UK Audit LLP, Baker Tilly Corporate Finance LLP and Baker Tilly Restructuring and Recovery LLP are limited liability partnerships registered in England and Wales, with registered numbers OC325348, OC325350, OC325347 and OC325349 respectively. Baker Tilly Tax and Accounting Limited, Baker Tilly Revas Limited, Baker Tilly Management Limited, Baker Tilly Business Services Limited, Baker Tilly Audit Limited and Baker Tilly CF Limited are registered in England and Wales with numbers 6677561, 6463594, 3077999, 04066924, 04045321, 06555639 respectively. Baker Tilly Financial Management Limited and Baker Tilly Investment Solutions Limited are registered in England and Wales with numbers 03953153 and 02051492 respectively and are authorised and regulated by the Financial Conduct Authority, Financial Services Register numbers 0192618, and 0116457. All limited companies and limited liability partnerships are registered at 25 Farringdon Street, London, EC4A 4AB. For Baker Tilly Business Services Limited, Baker Tilly CF Limited, Baker Tilly Audit Limited, Baker Tilly Financial Management Limited and Baker Tilly Investment Solutions Limited the term 'Partner' refers to the title of senior employees, none of whom provide services on their own behalf.

1. 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
AEDO	Agricultural Extension Development Officers
AGD	Accountant Generals Department
DFID	Department for International Development
DPP	Democratic Progress Party
FIU	Financial Intelligence Unit
FTC	Foreign Currency Form
GoM	Government of Malawi
GRN	Goods received note
GWAN	Government Wide Area Network
HR	Human Resources
IDEA	Interactive Data Extraction and Analysis
IFMIS	Integrated Financial Management Information System
IMF	International Monetary Fund
IPS	International Procurement Services
MCA	Malawi College of Accountancy
MDF	Malawi Defence Force
MK	Malawi Kwacha
MCP	Malawi Congress Party
MP	Member of Parliament
MPS	Malawi Police Service
MSRP	Manufacturer’s Suggested Retail Price
NAO	National Audit Office of Malawi
NK	Not Known
ODPP	Office of Public Procurement
ORT	Other Recurring Transactions account
PFMA 2003	Public Finance Management Act 2003
PP	People’s Party
PV	Payment Vouchers
RBM	Reserve Bank of Malawi
RSA	Republic of South Africa
Soft-Tech	Soft-Tech Consulting Ltd
STR	Suspicious Transaction Report
TI 2013	Treasury Instruction 2013
TP / RP	Top Prima / Rummage Pace
UAE	United Arab Emirates
UK	United Kingdom
ZAR	South African Rand

2. Introduction

Baker Tilly Risk Advisory Services LLP (Baker Tilly) holds a framework contract to provide forensic and investigation audit services to the United Kingdom (UK) Department for International Development (DFID). In October 2013 Baker Tilly was asked by DFID to provide forensic and system security audit services to the Malawi National Audit Office (NAO) following a request for support from the Government of Malawi (GoM). This followed the discovery of irregularities 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 and beyond, as the ‘Cashgate’ scandal.

In response to these apparent irregularities, through the Auditor General, the GoM instructed a forensic audit of suspected misappropriations for the period 1 April 2013 to 30 September 2013. The purpose of the review was to establish the facts behind, and the veracity of, these allegations. At the time the misappropriations were thought to involve between 8 and 10 different Government Departments.

On 21st February 2014 we reported our findings and observations to the Auditor General. This report detailed a number of weaknesses and failings in the internal control framework that had allowed “Cashgate” to occur. We also reported on 16 cases that had been handed over to the Auditor General for onward transmission to the Malawi Law Enforcement Agencies.

This new report summarises our findings based on the 53 case files handed over to date. A detailed report has also been provided to the Malawi Law Enforcement Agencies to assist them in understanding the case files and to support further action as appropriate. This report therefore complements and updates our report dated 21 February 2014 and does not duplicate our earlier findings. It should therefore be read in conjunction with the February report.

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; the details have been referred to the relevant Law Enforcement Office of the Police and Anti-Corruption Bureau through the Office of the Auditor General.

3. Background

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

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. We should stress that we have not sought to re-perform the work carried out by Soft-Tech and the outputs of the Soft-Tech report have been relied upon, in part, to advise our work.

At the same time as the Soft-Tech review the Auditor General instructed that a comprehensive review, covering transactions and IFMIS related controls between 1 April 2013 and 30 September 2013, should be undertaken and that this should include deleted transactions. It is this review that Baker Tilly was commissioned to complete, on behalf of the Auditor General.

The agreed scope of our original work required us to:

- Identify 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 the case of businesses, their owners, shareholders, directors, etc.;
- Identify, if false, any forged or fraudulent supporting documents and accounting entries in the books and records (including IFMIS) of Government Ministries;
- Identify, quantify and evidence any potentially misappropriated funds;
- Provide information that could be utilized in support of any possible litigation process to reclaim funds that were inappropriately paid during this period, as well as for any civil or criminal prosecution of entities involved, should the government so decide;
- Identify any failures and weaknesses in internal control, including failures within procurement systems, that could have allowed breaches to occur 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 needed or agreed.

On 21 February 2014 we issued a Forensic Audit Report on Fraud and Mismanagement of Malawi Government Finances (the "February 2014" report). We reported therein that at least MK 13,671,396,751 of GoM funds had been identified as being potentially misappropriated. This figure had been arrived at using defined testing criteria and a detailed analysis of 11 of the main GoM bank accounts. The review identified both 'Cashgate' and non-Cashgate transactions. In this context non-Cashgate items were noted as transactions that related to unsupported payments and/or poor procurements.

The report identified payments to 16 companies, valued at MK 6,096,490,705, where no evidence had been provided to support the provision of goods or services in relation to the payments made. As such MK 6,096,490,705 was classified as potential theft of Government Funds which should be the subject of appropriate legal action. A further 50 companies were then identified for further detailed work.

Our Audit work also identified high value payments made to two newly formed companies. The contracts awarded did not appear to represent value for money and price verification with other suppliers enabled us to identify MK 3,619,539,979 that, at best had been spent inappropriately or at worst, had been stolen.

Additional payments totalling MK 3,955,366,067 were also made to the same two companies. At the time of our February 2014 report no supporting evidence had been provided in relation to these payments.

Our previous findings can be summarised as follows:

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%

In the above context, in our February 2014 report, we stated that:

- the on-going nature of this investigation and the desire to issue this report would mean 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
- the figures relating to unsupported and poor procurement include transactions covering the periods 2012 to 2013.

We concluded that significant control failures and lack of application of the existing internal controls were key factors that had contributed to the failures and to the probable 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, 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, suggested that there could be no guarantee or assurances that future occurrences would not happen regardless of any control improvements implemented.

The relevant regulatory authorities should investigate the role of the banks in the cases where large sums of money were being deposited and then withdrawn to assess whether it would have been reasonable to expect the banks to raise concerns. If it is concluded that the banks had not acted in accordance with banking norms and related legislation appropriate action should therefore be taken.

Our previous report included 62 recommendations for improvement. At this stage we have not undertaken any follow up action on these 62 recommendations. There remains a need, therefore, to ensure that these recommendations have been implemented effectively.

This new report summarises our findings based on the 53 case files handed over to date. Each case file relates to one or more organisations that have been in receipt of government funding including all of the transactions deleted from IFMIS. Each case file has been referred to the relevant Law Enforcement Agencies through the Auditor General's office.

4. Scope of the Review

A total of 53 case files have been referred to the Auditor General. These cases are of varying complexity but as a minimum, each file considered and provided details on:

- Company formation documents;
- Any documentation to support the payment, invoices, pro-forma invoices, payment documents, contracts etc.;
- Identification of linked companies;
- Information on the company owners;
- Details of any Office of the Director Public Procurement records and associated correspondence;
- The Soft Tech deleted transaction report;
- Extracts from the GoM bank statements;
- Bank account application forms provided by the commercial banks;
- Authorised signatures for the accounts held;
- Details of all known bank accounts;
- Bank statements analysed back to January 2012;
- Cheque images or details of electronic funds transactions;
- Related party transactions;
- Funds deposit and withdrawal slips;
- Links with government employees;
- Company relationships;
- Interview notes (where appropriate);
- Details of any communications with the bank and supplier;
- Findings from Malawi Revenue Authority;
- Summary information provided by ACB;
- Identification of assets purchased, where necessary referring these to the ACB;
- Where appropriate and possible (without jeopardising on-going cases) visiting suppliers to obtain supporting evidence of spend;
- Details of our work with the Financial Intelligence Unit to trace overseas payments;
- Details of our work with international suppliers to benchmark product pricing and verify supply; and
- Any other information identified that may help in a successful prosecution.

In addition we have undertaken an IT systems security review and undertaken follow up activity to ensure the progression of those case files which we handed over in February 2014.

5. Summary of Findings

We have now completed our work on Cashgate related transactions focusing on the period 1 April 2013 to 30 September 2013. A total of 66 businesses were selected as part of our testing criteria and 53 cases have been handed over. Of these 48 relate to Cashgate. No further work was required for four cases and three were identified as duplicates. A further six non Cashgate related cases have been highlighted as requiring further work.

We have undertaken a detailed analysis of 63 bank accounts relating to the 53 businesses. In doing so we have identified 202 individuals who, either knowing or unknowingly, have been recipients of GoM funds. The 53 case files relating to these businesses, listing all of these individuals, have been handed over to the Auditor General for onward secure transmission to the relevant Malawi Law Enforcement Agencies.

This report is based on findings which were derived from the application of selection criteria similar to the nature of transactions that had been deleted along with transactions we considered to be higher risk. In this regard we consider that our work has included all lines of available supporting evidence, including third party verification where deemed appropriate.

As mentioned in our previous report we found that two main methods of misappropriation appear to have been used. The first focussed on the extraction of 'cash' (with the main currency being that of Malawi Kwacha) using systematic money laundering activities through commercial organisations. This would appear to have been premeditated and was not opportunistic. It is linked to what is commonly referred to as "Cashgate" and a number of GoM Civil Servants and other individuals, including some who stood predominantly as Independent candidates in the 2014 Malawi General Elections, are linked to these payments

The second method appears to be separate to the 'Cashgate' affair although the beneficiaries include some of the same companies. This suggests a crossover between the two methods. The payments in this "category" are part of a wider corruption scandal that focuses on high value, overpriced transactions and/or payments being made for goods not received, with funding transferred internationally to overseas jurisdictions into foreign currencies such as USD and ZAR. These transactions were relatively simple in nature including, inter alia:

- The overvaluing of goods whilst, obtaining quotations from genuine suppliers,
- Excluding ODPP from the procurement process; and
- Making fraudulent payments on quotation with no evidence of delivery.

The nature of these transactions suggests a combination of possible causes ranging from incompetence and/or professional negligence on the part of senior GoM officials, through to collusion between the various companies and/or individuals. Appropriate disciplinary and/or legal action should therefore be considered in relation to these employees.

The evidence also suggests that these cases, which occurred before Cashgate, involve larger sums of money whilst their nature must also give rise to a relatively high probability that other cases have occurred that have not yet been identified.

The transactions that we have identified as falling into this second category relate primarily to procurements made by the Malawi Defence Force and the Malawi Police Force. At the time of this report it is disappointing to report that we are still awaiting some of the financial information that we requested in relation to these transactions. In the absence of direct evidence the approvers of these payments should be subject to legal and recovery action in line with Treasury Instruction 2013 and Public Finance Management Act.

A summary of the losses and values at risk that we have identified, based on the 53 cases files handed over, is shown below.

No.	Description of ineligible expenditure	Feb-14 Amount MK	Add. Exp MK	Sep-14 Amount MK
1	Cashgate related deleted transactions	6,096,490,705	817,896,023	6,914,386,728
2	Cashgate related not deleted transactions	-	1,303,517,064	1,303,517,064
3	Inflated procurement prices / overpayment	3,619,539,979	233,223,617	3,852,763,596
4	Payment no supply	-	1,921,028,000	1,921,028,000
5	Overpayment (due for immediate recovery)	-	1,012,542,267	1,012,542,267
6	Scania Buses	-	520,000,000	520,000,000
	Ineligible expenditure	9,716,030,684	5,808,206,971	15,524,237,655
7	At risk no supporting evidence provided	3,955,366,067	564,267,679	4,519,633,746
8	At risk overpayment	-	332,587,198	332,587,198
	At risk expenditure	3,955,366,067	896,854,877	4,852,220,944
	Totals	13,671,396,751	6,705,061,848	20,376,458,599
9	At risk (FTC bounced transfers) Further supporting evidence required	-	3,915,007,791	3,915,007,791
	At risk further evidence required	-	3,915,007,791	3,915,007,791

This table above shows that the total loss suffered by the GoM has increased from MK 13,671,396,751 to MK 15,524,237,655.

The increase in the total identified loss figure relates to:

- An increase in the number of original Cashgate cases subject to comprehensive review, from 16 to 48. This is because those businesses receiving the highest value cheques were targeted first in the original report. We have now reviewed other companies:
- Confirmed valuation of overpriced items with insufficient evidence provided;
- Payments in respect of Scania Buses.
- Payments made for goods and services where no supply could be confirmed; and
- Payments made to the same supplier more than once for what appears to be the same invoice.

We have identified MK 4,852,220,944 which we have classified as 'at risk'. This figure includes:

- Payments made by the Malawi Police Service to two companies which were outside the scope of the review. However the similar nature of goods and descriptions on invoices would

suggest that these transactions should be subject to further investigation as they may be irregular; and

- Goods or services supplied where the values paid would seem to be overvalued. In this context as insufficient evidence has been made available to enable us to accurately value the loss we have conservatively estimated the "at risk" amount to be 50% of the total contract value;

We strongly recommend that a number of payments and procurements made by the Malawi Defence Force and by the Malawi Police Force require further comprehensive audit work to be undertaken, at the earliest opportunity, in order to verify whether an amount of MK 4,519,633,746 has been misappropriated.

An amount of MK 3,915,007,791 relates to foreign currency transactions where the payment would seem to have been returned due to incorrect bank account information though we should stress that foreign currency differences make understanding the accurate position challenging. At the time of this report insufficient evidence has been provided to enable us to confirm if these payments are valid and/or correct though anecdotal evidence would suggest that the explanations provided are reasonable and, therefore, that this aspect of the expenditure is valid..

Specific Cashgate Related Findings

A total of 104 Government cheques, valued at MK 6,914,386,728, were paid to 39 companies but for which no goods or services can be traced. We identified further payments noted as 'deposits' with similar characteristics to Cashgate payments in the various bank accounts of these 39 businesses. Here again no evidence of supply was identified to support these payments.

Further accounting entries were found to have been deleted for more cheques that would have been payable to Cashgate business although these were not banked. Four of the businesses did not bank the prepared cheques, valued at MK 430,000,000. We also identified relationships that existed between the various owners of these businesses; the interlinked nature of these businesses would suggest that the owners were made aware the Cashgate fraud had been uncovered leading them to refrain from banking any further cheques.

Four individuals were noted as being the main beneficiary of ineligible funds. One owner was linked to at least 18 businesses with two of these businesses receiving a total of MK 4,428,316,582 in 17 cheques. We also noted apparently unrelated individuals receiving or making payments into unrelated companies. Evidence of 13 individuals with links to the GoM and to the Cashgate businesses was also found whilst as part of this work we Identified businesses linked to nine individuals (or close relatives)

listed in the Malawi Electoral Commission (MEC) List of Parliamentary Candidates 2014 Tripartite Elections.

Using bank statements provided for the period 1 April 2013 to 13 October 2013 we identified that a total of MK 7,354,818,077 was withdrawn in cash from businesses linked to Cashgate. Almost half (48%) of this (MK 3,513,898,540) was withdrawn over a period of ten days. The largest single day for withdrawal of funds was Thursday 5 September 2013, when MK 827,647,000, in cash, was withdrawn. This amount represented 11% of the total cash withdrawn and MK 751,367,000 was withdrawn from various branches of one bank. One company withdrew a total of MK 550,000,000 on that date. It should be noted the most popular denomination of notes withdrawn were MK 1,000 and MK 500. Unfortunately not all of the commercial banks record the serial numbers of the batches of new bank notes they receive from the RBM making the tracing of bank notes difficult.

Whilst not of direct relevance to our findings if stacked on top of each other, 550,000 notes of MK 1,000 denomination would give rise to a tower of bank notes over 400 feet high. This graphically illustrates the scale of cash withdrawn, in just one day, by just one business.

We therefore believe that Cashgate was a pre-planned event. In addition to groupings of business we noted eight bank accounts which were opened just three months prior to receipt of high value GoM Cashgate funding.

Non Cashgate findings

Record keeping in relation to high value transactions was found to be unacceptable; we noted duplicate documentation; no or limited original documents; changes to values; the same document numbers being used for different procurements; and supporting documentation with an unacceptably poor level of detail. For example we found one payment for USD \$ 11,676,522 based on an invoice bearing the phrase "*for goods and services supplied*" where no further evidence to support the 'goods or services' could be located.

In addition we found that payments were regularly paid on proforma invoices. This is a declaration to sell and is not a true invoice. Payment should therefore never be made against proforma invoices.

We also noted the dual payment of one invoice resulting in the overpayment of USD \$ 3,100,500.

All of the above indicates the occurrence of significant internal control failures and could also indicate management overrides being applied in order to circumvent existing controls.

Our work identified four companies who successfully benefited from contracts with the Malawi Police Service (MPS) and the Malawi Defence Force (MDF) for which MK 15,553,562,598 was paid with either limited supporting evidence of supply or no evidence at all. Moreover no bank guarantees were obtained where advance funding was provided and no evidence to support any attempt to recover the values paid has been made. No evidence of action taken to debar the suppliers or prohibit them for bidding for government work in future could be found.

We also found that the same documentation, obtained from a genuine supplier, was presented on two occasions in different currencies; both were paid with no supply. The genuine supplier has confirmed that the goods would require arms release certificates and require multi jurisdiction approval prior to shipment. No evidence of this, or customs documentation relating to the shipment, could be traced. Documents provided suggest that these funds have been remitted to South Africa.

Further documentation made available to the audit team shows that the GoM made at least 14 payments to two businesses based in Hong Kong but also quoting a Hamriyah FZE address. Hamriyah Free Zone is located in Sharjah, United Arab Emirates (UAE). These payments total an estimated USD \$ 50,788,572.45 (MK 14,588,265,488) and were made into six different bank accounts.

It should be noted that actual payment relating to four of these documents (MK 3,915,007,791) can either not be traced to the Malawi Government Bank Accounts or relates to returned FTCs caused by incorrect banking information and includes payment made to different banks using the same FTC number.

We found that one company was formed in April 2012 receiving its first government contract just two months later. In this regard a number of issues were noted:

- No official registration details of this company could be traced.
- No due diligence into the company appeared to have been undertaken.
- Neither this company, nor another involved in the supply, had a trading history in the supply of the goods being procured.
- No ODPP documents could be traced relating to the company
- No evidence of tendering or requests for proposals (RFPs) could be found

It is therefore not at all clear how the Government of Malawi selected this business as one with whom to place significant contracts.

The audit team physically verified two shipments relating to this contract and confirmed delivery of two other supplies with the United Nations and MRA. These goods have arrived in Malawi. However investigations into the price of the goods supplied would suggest the purchased items were significantly overvalued when compared against even higher quality substitutes. Additional evidence subsequently submitted by the MDF, to explain the overvalued payments, was found to be unacceptable and lacking in substance.

We believe that a similar overpricing issue has occurred with the purchase of other items. Unfortunately poor record keeping made it difficult to determine the actual content of the purchases such that we could accurately assess comparable prices. We believe, however, that in this case at least 50% of the purchase price is therefore at risk from overpayment being USD \$ 970,000.00 (MK 332,587,198). Further work will be required on these payments.

The high level of loss, perceived to be incurred through poor value procurement, would suggest that 'Cashgate' could be secondary to wider corruption.

Other issues arising

A matter of particular concern is that, during an unannounced adhoc IT Security Audit by a member of our team, our inspection of the firewall configuration indicated that the firewall settings had been changed to permit any outside connection. We also found that password controls had been disabled, and the connections to the IFMIS servers, that should have been routed through the network firewall, had bypassed the firewall. This represents a fundamental weakening of the internal control framework such that it would allow a situation similar to Cashgate to occur again. This matter is of particular concern given the high levels of funding applied to improving IFMIS, the server and virtual machine set up along with the monitoring related training given to Accountant General staff in May and September 2013. IT security will therefore require continual monitoring to ensure that a similar "lapse" does not recur in the future especially given that the failure to apply existing controls was a key factor in the theft and misappropriation of funds.

In our previous report we made 62 recommendations. It is not clear, at this stage, how many of these have been implemented. Notwithstanding this, the lack of accountability, allied to a failure to apply or detect compliance with the Public Finance Management Act (PFM) requirements, has in any case allowed what could be considered to be deliberate circumvention of the control framework.

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 currently is no

guarantee that future frauds would be prevented regardless of any control improvements implemented.

6. Limitations

To limit the risk of prejudicing any current or future legal action, this report deliberately does not comment on specific transactions, names or companies. We should also stress that Baker Tilly is under no obligation contractually to produce a report for public release. Our work is on behalf of the Auditor General and our responsibility is to report our findings to him. It is for the Auditor General to decide on what, if anything should be made public at each stage in the process, in line with the Public Audit Act Sections 14 and 15.

Where we believe fraud, theft or unethical actions have taken place these have been referred to the relevant Law Enforcement Office of the Police and Anti-Corruption Bureau through the Office of the Auditor General. We should stress that this should not be taken to imply that those included in this report or the case files have committed any crime. This is for the legal system and the courts to determine.

Case files have been produced to support on-going legal action. As such they should be seen to support and not replace prosecution cases. Insofar as this report refers to matters of law, it should not be taken as expressing any formal opinion whatsoever.

The focus of our work related to the funds managed by the Government of Malawi, unless necessarily required otherwise. 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. In this regard the audit sample of 501 transactions was selected based on our risk criteria and does not include all transactions that the GoM processed between April and September 2013.

Our assessment is also 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. We should stress, however, that there will be documents and information that may exist which we have been unable to locate, and/or which were not handed to us or were not provided in the time that was available to us.

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. This report is, from necessity, 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.

The findings expressed in this report are therefore 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. In this regard 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, however, not all requested information has been provided by the various bodies with whom we interacted.

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.

Report

Upon delivery of this report to the Auditor General, the Auditor General will assume full responsibility for the report and its contents.

7. Quantification of loss

7.1. Quantification of Loss to the Government of Malawi

Initial scoping work using the Soft Tech report identified 66 cases of which 48 related to Cashgate, five related to additional cases identified from analysis of 11 of the GoM main bank accounts and three cases were duplicates¹. Six of the remaining ten cases were classified as high risk and identified as requiring further work. These are not Cashgate related and the values at risk have not, as yet, been identified. On the four remaining cases we recommend that no further work is appropriate.

A summary of the status of the 66 cases is shown below:

No.	Detail	Amount	Amount %
1	Cashgate cases	48	73%
2	Additional cases identified from main 11 GoM bank accounts	5	8%
Total cases handed over to date		53	80%
3	Duplicate cases	3	5%
4	Six cases where further work required	6	9%
5	No further work required	4	6%
Total cases initially identified		66	100%

53 case files (48 'Cashgate' and 5 additional cases) have been handed to the Auditor General for secure onward transmission to the law enforcement agencies. This summary report is based on the findings from these 53 cases and concludes our work on Cashgate related cases.

We have identified a loss to the Malawi Government of MK 15,524,237,735. A summary of the losses identified to date, based on the 53 case files handed over, is shown overleaf. We also see substantial value in the completion of the remaining six remaining cases.

A further MK 8,767,228,735 has been classified as 'at risk'. This relates to payments where we have been unable to obtain sufficient evidence in the time period and additional work will be required to verify these payments by the Government of Malawi.

¹ Please note the Soft Tech report highlighted 72 cases of which 10 were duplicates and 14 were deemed to be accidental deletions due to their proximity to the Cashgate cases. No further work was completed on these 14 cases.

No. Description of ineligible expenditure	Feb-14 Amount MK	Add. Exp MK	Sep-14 Amount MK
1 Cashgate related deleted transactions	6,096,490,705	817,896,023	6,914,386,728
2 Cashgate related not deleted transactions	-	1,303,517,064	1,303,517,064
3 Inflated procurement prices / overpayment	3,619,539,979	233,223,617	3,852,763,596
4 Payment no supply	-	1,921,028,000	1,921,028,000
5 Overpayment (due for immediate recovery)	-	1,012,542,267	1,012,542,267
6 Scania Buses	-	520,000,000	520,000,000
Ineligible expenditure	9,716,030,684	5,808,206,971	15,524,237,655
7 At risk (FTC bounced transfers)	-	3,915,007,791	3,915,007,791
8 At risk no supporting evidence provided	3,955,366,067	564,267,679	4,519,633,746
9 At risk overpayment	-	332,587,198	332,587,198
At risk expenditure	3,955,366,067	4,811,862,668	8,767,228,735
Totals	13,671,396,751	10,620,069,639	24,291,466,390

Paragraphs 6.2- 6.9 contain more information on each of the different categories shown above.

7.2. Cashgate related deleted transactions

In total 104 GoM cheques, totalling MK 6,914,386,728, were paid to 39 different companies without them appearing to supply any legitimate goods or services in return. Soft Tech identified that accounting entries for the majority of these transactions had been deleted from IFMIS.

The Soft Tech report identified 48 companies that may have received Cashgate funds. Following a review of the bank statements for these businesses (where they could be obtained) it was found that nine businesses did not bank any Cashgate cheques. Two of these companies did, however, receive payments that we considered to be ineligible but these do not appear to be 'Cashgate' related.

7.3. Cashgate related "not deleted" transactions

We identified 32 cheques, totalling MK 1,302,517,064, that had been paid to 18 different companies with characteristics of 'Cashgate' but for which no supporting evidence could be located. The accounting entries for these transactions were not deleted as per the Soft Tech report.

Further analysis of the 32 cheques showed that the largest cheque payment was for MK 349,568,231, the lowest cheque payment was MK 216,795 and the average cheque value was MK 39,510,715. These cases have been referred to the ACB for follow up and recovery action as appropriate.

7.4. Inflated procurement prices / overpayments

The report issued in February 2014 originally identified MK 7,574,906,046 as being unsupported payments or losses arising from poor procurement practices. These loss types have now been split into further categories to better reflect the nature of the transactions. More details are provided later in this report. For the purpose of this report, and based on independent price verification, MK 3,852,763,596 has been identified as arising from inflated procurement prices and overpayments.

7.5. Payments where no supply has been made

MK 1,921,028,000 has been identified that relates to payments made where there is no evidence either internally or by third party of any supply.

7.6. Overpayments

Payments for invoices for goods and services that have been duplicated and paid more than once should be subject to immediate recovery. Action should be taken to recover payments, valued at MK 1,012,542,267, with immediate effect.

7.7. Scania Buses

The value includes an unauthorised payment for MK 520,000,000 in relation to six Scania buses.

7.8. At Risk Expenditure

Payments totalling MK 8,767,228,735 will require further investigation by the Government of Malawi. These include foreign currency transaction documents that cannot be traced and payments on behalf of the Malawi Police Service that were outside the scope of this assignment.

7.9. Un-cashed cheques relating to Cashgate "deleted" transactions

We noted 22 payments, totalling MK 1,185,657,562 allocated to 15 different companies, for which the accounting entries had been deleted. No evidence of these cheques being banked could be traced (as at August 2014).

8. Review of 'Cashgate' cheques

104 'Cashgate' cheques were paid into at least ten different commercial banks throughout Malawi with 22 cheques, linked to 10 different businesses, being banked at one bank. These 22 cheques represent 49% of the 'Cashgate' funds. Analysis of the 22 cheques deposited into one bank shows that the majority of this related to two businesses who received MK 1,860,584,273 and MK 1,140,738,209, respectively. These amounts total MK 3,001,322,482 representing 43% of the total 'Cashgate' cheques. Both businesses are owned by one individual.

The second and third highest cheque amounts were deposited in to NBM and FDH Bank being MK 970,620,798 and MK 898,276,664, respectively. NBM was also the bank into which the highest number of Cashgate cheques were deposited (28 out of 104) and the bank with which the highest number of businesses who were recipients of Cashgate cheques held bank accounts (12 out of 39).

In summary, the three banks in to which the majority of the Cashgate funds were deposited between them received MK 5,219,344,243 (75.5%) of "Cashgate funds". The remaining 24.5% was split between at least seven different banks.

Ten businesses received MK 5,356,552,249 which is equivalent to 78% of the total 'Cashgate' funds. Of these, three businesses owned by two individuals, received a total of MK 3,730,784,085 being 54% of the total value of the Cashgate cheques.

A full report with the details of all of the above transactions has been provided to the Auditor General.

9. Review of 'procurement fraud' payments

In addition to the Cashgate businesses, the bank statements of the main 11 GoM bank accounts were reviewed for high value and duplicate payments. A number of payments, with these characteristics, were noted as being paid from the Malawi Defence Force (MDF) bank account. These payments met the pre-determined audit criteria for sample testing large payments (> MK 90m).

Our work identified 17 payments, totalling MK 16,639,897,577, to six businesses where no supply or limited supply of goods could be evidenced. The accounting entries for these transactions were not deleted from IFMIS. One business received MK 1,043,857,475 in three cheque payments from the GoM via the MDF. The MDF confirmed that it did not receive any goods, services or works with regard to at least MK 805,015,000 of this amount. A further two cheques, totalling MK 400,000,000, were also found to have been paid to the same business with no supporting documents to prove evidence of supply whilst an invoice, payable to the same business for MK 32,707,375, has been paid twice.

One business received MK 920,000,000 in August 2013 from the MDF for specialist items. No evidence could be provided by the MDF or MRA to support delivery. A price comparison exercise found the unit prices to be inflated by at least 2.3 times the average market price of the goods. This business made an onward payment of MK 480,000,000 to a linked business; the majority of the funds were then withdrawn in cash. A further payment of ZAR 30,000,000 (equivalent to MK 1,001,028,000) for the same specialist items was made. Similarly no evidence of the supply or delivery of the goods for this payment could be provided by the MDF. The files provided by MDF contained no correspondence indicating that any legal advice had been sought to assist in reclaiming the amounts paid.

The originating supplier of the specialist items has confirmed that they have never supplied MDF, or the business in question, although they had provided quotations in both USD and ZAR to the MDF. An analysis of the business bank accounts would suggest that no goods or services of any reasonable value similar to those the business was engaged to procure, have been purchased. As such we believe these purchases to be fictitious and, therefore, fraudulent.

The documentation made available to us suggests two businesses are related and the GoM made at least 14 payments totalling an estimated USD \$ 50,788,572.45 (MK 14,588,265,488). In this regard it should be noted that actual payment relating to four of these documents can either not be traced to the Malawi Government Account or relates to returned FTCs caused by incorrect banking information. As such four transactions to the value at MK 3,915,007,791 require further investigation and have been classified as 'at risk FTC Bounced Transfers'.

In relation to the above transactions we have only been able to trace one of the two related businesses in global company registration records; however we believe these two businesses are related. An individual with the same surname as the director of the traced company uses the same address as that quoted on invoices submitted and this would suggest a family link between the businesses.

The remaining confirmed payments obtained from Foreign Currency Transfer Forms notes total MK 10,673,257,697 and were paid by the Malawi Defence Force (MK 5,979,039,979) and Malawi Police Service (MPS) (MK 4,694,217,718). No work has been undertaken on the payments to MPS as these were considered to be not Cashgate and out of scope. We have therefore recommended that work commences to review these cases as a matter of priority.

The payments relate to Parka Jackets, Riot Control Equipment and Combat Uniforms. A similar payment was noted for Anti-Riot gear funded by MDF, for a similar value, both benefiting one of the companies. It should be noted that the MPS payment for Anti-Riot Gear was to be paid on behalf of another supplier; it was not clear to us why the MPS would make payment on behalf of another company. As such the remaining value of MK 3,125,347,021 is classified as 'At Risk No Supporting evidence'. Further work will be required on these payments.

Four payments totalling USD \$ 16,366,000 (MK 5,313,865,583.20) were made via three bank accounts to supply military related items. Supporting documentation suggests that the payments relate to four shipments made between the 14 November 2013 and 17 January 2014. We physically verified two shipments and confirmed that the remaining two were reflected on both United Nations Registers and MRA customs documentation.

We believe, however, that an overpricing issue has occurred with the purchase of other military hardware. Unfortunately poor record keeping made it difficult to determine the actual content of the kits such that we could make price comparisons. . We believe that at least 50% of the purchase price is at risk from overpayment being USD \$ 970,000 (MK 332,587,198).

A summary of the different types of loss associated with these two businesses is shown below:

Loss Type	MDF MK	MPS MK	Total MK
Over payment	3,852,763,596	-	3,852,763,596
Over payment to Recover	-	979,834,892	979,834,892
Ineligible payments	3,852,763,596	979,834,892	4,832,598,488
At Risk (FTC Bounced Transfers)	3,325,971,986	589,035,805	3,915,007,791
At Risk No Supporting Evidence Provided	-	3,125,347,021	3,125,347,021
At Risk Overpayment	332,587,198	-	332,587,198
Payments at risk	3,658,559,184	3,714,382,826	7,372,942,010
Total	7,511,322,780	4,694,217,718	12,205,540,498

In completing this aspect of our work we considered the quality of record keeping and documentation to be wholly unacceptable. For example we noted;

- Duplicate documentation;
- Cases where no original documentation (or at best limited documentation) could be found;
- Cases of values changing for no apparent reason;
- Cases where the same document numbers had been used for different procurements;
- Supporting documentation with an unacceptably low level of detail i.e. a payment for USD 11,676,522 based on an invoice for 'goods and services supplied' no further evidence to support those 'goods or services' can be supplied.
- Payments being made on proforma invoices. A proforma invoice is a declaration to sell and is not a true invoice. Payment should not be made against invoices of this nature in the absence of a bank guarantee.

One company examined had been formed in Hong Kong on 1 April 2012. On 8 June 2012 proforma invoices were issued to the MDF to supply military equipment, and on the 4 September 2012 two payments were made through Foreign Currency Transfers

In reviewing this company we found that

- No evidence of due diligence on this company, prior to contract award could be traced.

- No Bank Guarantees had been provided.
- The company had no trading history in the supply of goods procured.
- No evidence of tendering or requests for proposal has been noted.
- No ODPP documents could be traced.
- Limited evidence of supply could be located

It is therefore unclear how the Government of Malawi selected this business as one with whom to place material contracts.

We have also undertaken work to verify and benchmark the price of the military equipment and believe the estimate of USD \$ 1,500 per unit as quoted in our February report to be an accurate reflection. In the absence of any competitive international tender and linked to the restrictive single source tendering we believe that these purchases are in excess of their true cost. As such the GoM has potentially overpaid by USD \$ 11,866,000 (MK 3,852,763,596).

Similar observations related to a second company covered by our review. In this instance, between 23 October 2012 and 21 August 2013, the GoM made five payments totalling at least MK 5,283,253,522 through Foreign Currency Transfers. Here again no Bank Guarantees were provided, no company due diligence was performed prior to payment and no ODPP documents could be traced whilst no evidence of tendering or requests for proposals could be found. Reference was, however, made to single source tendering approved by Ministers on 15 August 2012 for this procurement. This was somewhat surprising given that the company had no trading history in the sourcing and supply of the goods being procured.

In addition no evidence of shipment could be proved by MDF or MRA for goods provided by the company. In our opinion it is probably that this company is fictitious and all payments to it should be considered as fraudulent. Thus five payments, totalling MK 5,283,253,522, should be classified as theft of government funds unless evidence can be provided to the contrary.

The Auditor General has made two written requests, on our behalf, to the Financial Intelligence Unit to identify the beneficiaries' accounts in Dubai and Hong Kong for these two companies. At the time of this report we have received no formal response.

Finally in this regard we identified an invoice for USD \$ 3,100,500 for combat uniforms issued to the MPS. The document requests payment is split in two with 50% to the each bank. For reasons unknown two payments for USD \$ 3,100,500 have been made to each bank suggesting the payment

was not split as required. As such USD 43,100,500 (MK 979,834,892) has been overpaid and is due for immediate recovery.

The focus of our work on the two companies above relates solely to the transactions between MDF and the two businesses. Transactions with the MPS will therefore require further investigation.

10. Accounting Entries Deleted but Cheques Not Cashied

Analysis of the deleted accounting entries against the bank statements of the 'Cashgate' businesses found that accounting entries for 22 cheques, totalling MK 1,185,657,562, were deleted but that the cheques (if indeed they were ever printed) had not been cashed. These 22 cheques related to 15 different businesses.

A review of this data found a number of trends and patterns as set out below.

- The majority of the unpaid cheques were allocated against the Ministry of Irrigation & Water Development (14/22), then LGRD (6/22) and finally the Ministry of Tourism, Wildlife & Culture (2/22) with the cheques totaling MK 727,000,000, MK 433,600,894 and MK 25,056,668, respectively.
- The highest value unpaid cheque was to a company identified elsewhere as a Cashgate beneficiary for MK 396,458,744, the lowest value unpaid cheque was for MK 2,892,273 and the average unpaid cheque amount MK 79,043,837. The accounting entries related to the highest value unpaid cheques were the only entries deleted on 27 August 2013. Entries for the five other payments to the company were deleted on 3 September 2013. The cheque number is noted to be earlier in the sequence.
- The unpaid cheques for the top three businesses totaled MK 709,458,744 and represented 60% of the total unpaid cheques.
- The 14 cheques allocated to seven businesses in the Ministry of Irrigation & Water Development were made up of two payments for odd amounts that, when combined, equaled a round sum amount. This would suggest that the amounts to be paid to each company were pre-determined before being split into smaller, less obvious figures. It is not known why the cheques were never banked.

We also noted that there appeared to be relationships between the owners of five of the businesses linked to the unpaid cheques. For example we found that they had provided banking references for one another that they deposited and withdrew cash from one another's bank accounts, transferred funds between two of the businesses and that two of them are based at the same address. We also noted that four of these five businesses did not bank eight cheques totalling MK 430,000,000.

The inter-linked nature of these businesses would suggest that it is possible that the owners may have been tipped off that the 'Cashgate' fraud had been discovered and that they then sought to protect themselves by not depositing these cheques.

11. Payments to 'Cashgate' Businesses but Accounting Entry Not Deleted from IFMIS

A review of the bank statements for the Cashgate businesses found that other GoM receipts, with similar characteristics to the Cashgate cheques, had been banked. These "indicators" included cases where there were no supporting documents, duplicate amounts, the same cheque signatories, payments allocated against the same ministries and the cheque proceeds being withdrawn in cash.

In total 32 cheques, totalling MK 1,302,917,063, with these characteristics were paid to 18 businesses. The identification of these GoM payments suggests that not all of the accounting entries for potentially fraudulent payments made to these businesses were deleted.

The highest amount paid was MK 349,568,231 while the highest number of cheques issued was four. The majority of the cheques had been allocated against the Ministry of Tourism, Wildlife and Culture (MK 429,879,376) followed by the Ministry of Irrigation & Water Development (MK 137,675,469) and then the Ministry of LGRD (MK 79,059,152).

On the basis of the evidence provided, and unless any further supporting documents can be provided to prove the legitimacy of these payments, these payments should be included in any action taken to recover misappropriated funds.

12. GoM Cheque Signatories

We identified 104 cheques, totalling MK 6,914,386,728, paid to 39 businesses in relation to the 'Cashgate' element of the fraud. These 104 cheques were signed by six different individuals employed in the Accountant General's Department all of whom were Senior GoM Civil Servants.

Two individuals signed 96% and 90% of the cheques issued with the third most common signatory signing 64% of the cheques issued. The most common "*three signature combination*" was present on 65 of the 104 Cashgate cheques (63%). Unless signatures have been forged, these three individuals must have been aware of the amounts they were paying to specific businesses as an examination of the cheque numbers and dates shows that numerous sequentially numbered cheques from the same cheque books were issued to the same suppliers on the same dates.

We would have expected any Senior GoM Civil Servants, signing multiple cheques to the same businesses within a short time period, to have challenged these payments and to question why so many cheques were being written to the same businesses at the same time.

In this regard it is also of concern that we have been unable to trace any documentary evidence, such as quotations, email or letter correspondence, contracts, agreements, invoices or delivery notes between these businesses and the GoM, which would help establish the legitimacy of these transactions.

In our opinion the six individuals appear to have breached their fiduciary duties as detailed under Section 2.5 Responsibilities of Controlling Officers of the Treasury Instructions dated 1 May 2013. We therefore recommend that appropriate legal and disciplinary action should be considered against these six employees.

13. Controlling Individuals

Our work identified at least 202 individuals who have received the monies flowing from one or other of the different loss types described above. However a review of the 53 businesses shows that the majority of the ineligible funds identified were paid to four individuals who control seven different businesses.

- One owner is linked to at least 16 different businesses; the available evidence would suggest that two of these businesses received 'Cashgate' cheques. We further noted that transfers were made from these two businesses to at least two other businesses under their control. In total these companies received a total of MK 4,428,316,582 via 17 cheque payments from the GoM, without evidenced supply of goods, services or works in return.
- One business owner is linked to four different businesses and two of these businesses received MK 1,246,225,751 via six cheques from the GoM without supplying any goods, services or works in return. This individual is also a bank signatory for another Cashgate business although he also appears to use an alias.
- In the four month period between 1 May and 6 August 2013 one business owner banked six GoM cheques totaling MK 477,768,916. Examination of the cheque numbers showed that two sequentially numbered cheques were issued on three different dates at least a month apart. The accounting entries for both of the high value cheques had been deleted.

From the above analysis we concluded that, especially where the combined value of the 'Cashgate' cheques paid to businesses exceeds MK 200m, at best, the individuals that own these businesses have been used to launder GoM funds as they have received, deposited and withdrawn significant amounts of GoM funds.

It is of note that none of the individuals, into whose bank accounts 'Cashgate' funds were deposited, appear to have contacted the GoM or any law enforcement agencies to inform them that their bank accounts had been incorrectly credited with the funds or made any effort to repay the funds.

14. Links between businesses and parliamentary candidates

Following completion of the case files the names of the individuals linked to the businesses were researched and compared against the Malawi Electoral Commission (MEC) List of Parliamentary Candidates 2014 Tripartite Elections². This exercise identified nine individuals (or close relatives) who were listed as standing in the 2014 Malawi General Election and who appeared to have links to the businesses that received funds from the GoM without providing any goods, services or works in return.

One individual who ran for election is noted to have received MK 4,428,316,582 with the lowest amount being MK 16, 750,000. Four individuals are linked to a business that received in excess of MK 100,000,000.

These links would suggest the proceeds of Cashgate may have been used to support electoral campaigns though it is not possible to confirm the source of the funding.

² <http://www.orakonews.com/wp-content/uploads/2014/02/List-of-Parliamentary-Candidates-2014-TPE-Nomination-Results.pdf> (accessed on 2 June 2014)

15. 'Cashgate' businesses

We attempted to trace the names of the individuals who deposited or withdrew funds from those businesses that banked 'Cashgate' cheques with a view to identifying individuals with employment or personal links to the GoM.

Internet searches were conducted and enquiries made to establish current or past job roles of any individuals or family member with links to the GoM. This review enabled us to identify 13 individuals with possible links to the GoM. It is also likely that there are other individuals with no or limited internet 'footprint' that we have been unable to identify.

We also found that companies seemed to operate in a group, although the reasoning for this was not readily apparent, for example five individuals owned four different businesses that benefited and banked Cashgate cheques and all were found to have withdrawn funds from one of the companies. Three of the companies are noted to have had IFMIS accounting entries deleted but the cheques matching these amounts were never banked. Given the inter linked nature of these four businesses it is possible that the owners may have been tipped off that the 'Cashgate' fraud had been discovered and tried to protect themselves by not depositing these cheques.

In addition to the above we found that:

- Two individuals withdrew cash from various company accounts accompanied by the owner of the account.
- One individual deposited funds into three different companies. He was connected to only one of these companies.
- Owners of Cashgate recipient companies were acting as banking references for other Cashgate companies

16. Cheque Sequencing

Cheque Sequencing

Our analysis of 158 cheques issued by the Government of Malawi identified 44 gaps in the sequence of cheque numbers. Cheques had been written on 23 different dates. On each of these dates a new cheque sequence began. Therefore, even after eliminating the effect of 23 sequence gaps caused by a new date, there remain 21 cheques missing from the sequence. In total 137 (87%) of 158 cheques followed the sequence of cheque numbers.

This analysis would suggest that fraudulent cheques were written in batches and were sequential across certain dates from April – September 2013.

Cheque books used

The first cheque written on 2 August 2013 was cheque number 16131. The last cheque written on 26 August 2013 was cheque number 17510. The first cheque written on 7 June 2013 was cheque number 19947. If sequential cheques were being used properly we would expect the reference numbers used for June cheques to be lower than those in August. That is clearly not the case. This suggests that cheques are not being used, or generated, in sequential order making audit trails and reconciliations unnecessarily difficult.

We also found that there were 328 cheques missing from the sequence in which cheques were written. We recommend that these cheques are investigated to establish the legitimacy of the payments made. To assist in this process cheque scans should be obtained from the RBM and IFMIS reports should be examined in order to obtain details of these cheques.

Findings by date

We analysed cheques written on 23 different dates. Of these, one cheque dated from 2011 and is not thought to be related to Cashgate. Analysing 22 dates on which Cashgate cheques were written, we identified two dates where unusually high numbers of cheques were issued to a group of companies which, again, implies a level of re-planning and organisation

17. Cash withdrawals

Bank statement and cash withdrawal analysis was undertaken on those businesses depositing Cashgate cheques. We found several examples of very high withdrawals in the form of cash. The following paragraph focuses solely on cash withdrawals and does not include intercompany payments or cheque payments deposited into individuals' accounts.

Between the periods 1 April 2013 to 13 October 2013 a total of MK 7,354,818,077 was withdrawn in cash from businesses linked to Cashgate. Of this total, ten businesses withdrew MK 5,550,807,101.00 (75%). Of these we identified that one individual owned three of the businesses, and one person owned two businesses. We could also link two of these ten companies to Government of Malawi Officials.

Of the MK 7,354,818,077 withdrawn in cash over the period almost half (48%) (MK 3,513,898,540) was withdrawn over a period of ten days. This is shown in the table below:

	Date	Amount MK	% of total during period	
	Friday	26/07/2013	215,587,800	3%
	Thursday	15/08/2013	262,058,500	4%
	Thursday	29/08/2013	210,481,100	3%
	Friday	30/08/2013	358,618,165	5%
	Monday	02/09/2013	286,612,000	4%
	Tuesday	03/09/2013	607,970,000	8%
	Wednesday	04/09/2013	258,187,615	4%
	Thursday	05/09/2013	827,647,000	11%
	Friday	06/09/2013	264,083,000	4%
	Thursday	12/09/2013	222,653,360	3%
			3,513,898,540	
	All other dates 1/4/13 to 13/10/13:	3,840,919,537	52%	
	Total during period:	<u>7,354,818,077</u>		
	Sum shaded:	2,339,034,780	32%	

The most active period for cash withdrawals was the week from Friday 30 August to Friday 6 September 2013, during which MK 2,339,034,780 was withdrawn in cash, amounting to 32% of the total amount withdrawn in the 28 week period from 1 April 2013 – 13 October 2013. The largest single day for withdrawal of funds by cash was Thursday 5 September 2013, when MK 827,647,000 was withdrawn, being 11% of the total for the period.

The high level of withdrawals suggests a coordinated approach to withdrawing cash. It is also of note that, given the sums involved, one would normally expect advance requests to have had to be made to the RBM as we understand the amounts withdrawn would have led to some branches exceeding their daily insurance limits. We could find no evidence that these requests had been made.

The tables above and below demonstrate that, of the MK 827,647,000 withdrawn on 5 September 2013, the largest amounts were withdrawn from one bank. There were significantly more cash withdrawals from this bank's branches in Capital City, Ginnery Corner, Balaka, Lilongwe and City Mall than from any other commercial bank. One company withdrew MK 550,000,000 from the various branches on that date. Furthermore, on 5 September 2013, MK 220,137,000 was withdrawn in cash from the banks' Capital City branch. The bank is unable to provide the serial numbers for the batches of new bank notes they receive from the RBM making the tracing of notes difficult if not impossible. This bank had the largest volume of withdrawals of cash linked to Cashgate, being MK 3,809,317,251 or 52% of the total. The largest withdrawals were made by two businesses owned by the same person. In this regard over the period 1 April 2013 to 13 October 2013 MK 2,702,687,842 or 37% was withdrawn by one business.

Whilst not of direct relevance to our findings it is an interesting and illuminating fact that, if stacked on top of each other, 550,000 notes of MK 1,000 denomination would give rise to a tower of bank notes almost 400 feet high and weigh 550kg. This, graphically illustrates the scale of cash withdrawn, in just one day, by just one company.

The relevant regulatory authorities should investigate the role of the banks in these cases to assess whether it would have been reasonable to expect the banks to raise concerns at the very large sums of money being deposited and then withdrawn. If it is concluded that the banks had not acted in accordance with banking norms and related legislation appropriate action should be taken.

Malawi Kwacha has a limited tradable market outside of Malawi. It is therefore unclear what has happened to the cash withdrawn. However the release of huge sums of bank notes by the banks without recording serial numbers makes continued tracing very difficult. Further asset tracing will therefore be required if one is to gain a better understanding of what happened to these funds.

18. Bank Accounts Opened Prior to Receiving 'Cashgate' Funds

An examination of the bank mandates for the 'Cashgate' businesses identified four business registered or incorporated between 22 May 2014 and 6 August 2014. These companies received MK 677,383,680. The information available suggests that, in all practical respects, the timing is such that these businesses would have been unable to compete for Government contracts in the period between formation and successful engagement. We therefore believe it very likely that the companies had been formed for the sole purpose of receiving Cashgate funds.

A further four businesses opened bank accounts between 8 April 2013 and 20 August 2013. Within three months MK 429,817,180 had deposited.

One further company opened a bank account to deposit GoM cheques but no activity was noted.

We also found cases of dormant bank accounts being re-opened. Taken together the opening of new bank accounts and the re-opening of dormant bank accounts, closely followed by the depositing of large value GoM cheques within relatively short periods of time, suggests that these were premeditated actions taken to in order to defraud the GoM.

We could not locate any Suspicious Transaction Reports (STR's) being raised by the commercial banks in relation to these cheque deposits. This would suggest a low level of STR compliance - and the latter should act as a key control over large scale fraud and money laundering.

19. Transfers between Cashgate businesses

Examination of the bank statements and cheque images for the 53 companies reviewed identified 13 transfers, greater than MK 1,000,000 between the different businesses. A further three transfers between one of the 53 businesses and their related group businesses were also traced. The total value of the 16 transfers was MK 1,021,744,761.

To date no documentation demonstrating that these 16 transfers were for legitimate business purposes has been provided. We therefore recommend that further work is undertaken to establish their business purpose, if any.

Ten of the 13 transfers, totalling MK 950,894,000, were to one business which received funds from three different businesses. No paperwork was available to show what goods, services or works were supplied.

Eight of the 10 transfers were between companies controlled by the same person. Two transfers were also noted to be between companies owned by another individual who was the second highest recipient of Cashgate funds. These two individuals are either the ultimate beneficiaries or appear to have been trusted to receive, transfer and withdraw large amounts of ineligible funds through their private businesses.

Individual bank statements show that funds were then withdrawn in cash following receipt of these transfers. High value transfers followed by rapid cash withdrawals from the final beneficiary is a clear indicator that a business is being used as a conduit to process the proceeds of a crime and is normally part of the layering process to launder funds.

In this regard layering is the process of engaging in a series of conversions or movements of funds to distance them from their source and mask their origin. In some instances, the "launderer" might disguise the transfers as payments for goods or services, in an attempt to give them a legitimate appearance. It is therefore important that the Malawian law enforcement agencies confirm whether or not the transactions had any genuine business purpose.

20. Payments to legal practitioners in Malawi

Our review identified four payments, totalling MK 140,896,121, to three different legal practitioners in Malawi, made between July and September 2013. All were made using 'Cashgate' funds. All three are listed as licensed legal practitioners for the period 1 February 2014 to 31 January 2015 on the Malawi Law Society website. We therefore recommend that the ACB confirms whether or not all three businesses were licensed in the previous year at the point when they received these payments.

Further work should also be undertaken to establish the reasons for all four payments and a review of the money laundering checks completed by these solicitors prior to them receiving the funds, should be completed by the ACB. Where breaches are identified the Malawi Law Society should be informed.

21. Businesses registered in 2013

A review of the bank registration documents identified three businesses registered in 2013. The businesses received a total of MK 569,712,229. In our opinion it is very probable that these businesses were formed specifically to act as conduits to receive GoM funds.

Audit work found no evidence of goods; services or works have been provided in return for the payments. No evidence of approval for supply has been provided by ODPP.

22. Withholding Tax

We reviewed 31 "Withholding Tax certificate books" for the period 11 March 2013 to 14 November 2013. We were not able to trace withholding tax certificates for a high proportion of payments that, if legitimate, should have been subjected to withholding tax at source. The payments made to these businesses suggest that no tax was deducted which calls into question the legitimacy of the payments received from the GoM.

Conversely should these payments be identified as legitimate the MRA should undertake immediate investigation and recovery action. Moreover, the decision not to deduct withholding tax at source would further suggest collusion between the companies and government officials.

23. CASH WITHDRAWALS IN USD

Individuals relating to four businesses were found to have withdrawn funds in US Dollars through various bank accounts. These withdrawals totalled USD 92,354 (MK 29,636,040) as follows:

	USD	MK Equivalent
Company 1	45,000.00	12,139,728.00
Company 2	2,354.00	819,611.00
Company 3	25,000.00	9,248,541.00
Company 4	20,000.00	7,428,160.00
	<u>92,354.00</u>	<u>29,636,040.00</u>

On two occasions the supporting documentation suggests that the funds related to overseas business trips. However we found that the individuals supposedly travelling overseas continued to make use of ATM machines during and after the period they were purported to be overseas suggesting that the business trips may not have happened although it is possible that someone else was using the ATMs on their behalf.

We were unable to trace funds converted outside the normal banking system.

24. Information Systems Review

During August 2014 we performed an unannounced spot check audit, with respect to the Information Systems ('IS') Control Environment at the Office of the Accountant General of the Malawi Government. Our work was performed in accordance with the International Standard on Related Services applicable to agreed-upon procedures engagements. The complete IS control environment located at the Office of the Accountant General of the Malawi Government was not evaluated.

Our detailed findings have been submitted in a separate report to the Auditor General. As a result of this work we are concerned that the potential for "Cashgate" to happen again remains a very real possibility owing to significant weaknesses in the IT control environment.

Of particular concern are the connections to the IFMIS servers that should go through the network firewall. Inspection of the cabling connected to and from the firewall indicated that a connection from the Disaster recover site had bypassed the firewall and had been connected directly to the router. This was possible because the firewall housing is broken and not secured; As a result individuals with access to the server room have the ability to bypass the firewall connections to the IFMIS servers.

Inspection of the firewall configuration indicated that the firewall was set to permit any outside connection. The IT consultant indicated that this was not supposed to be the setting and that it had been changed. We were unable to identify the person who changed this setting. The ability to change the firewall configuration requires access to the firewall password and the users with this password knowledge were also unknown.

As a result of our work the IT consultant changed the setting to deny outside access and changed the password to prevent unauthorised access. This will require continual monitoring.

Access to the server is restricted via a numeric key pad (pin required) but this is dependent on a stable power connection. Should there be a power failure and the generator fail to switch on, the server room has no access restriction. We also found that there is currently no monitoring of server room visits granted to IT Staff or to external visitors.

Upon inspection of the server room the following was noted:-

- There are no temperature and humidity sensors.
- The air-conditioner around the IFMIS servers was not working which resulted in the internal cooling fans on the servers running exceptionally high.

- Dust regularly accumulates around the server infrastructure as is not adequately removed.

Inspection of the server room also indicated that network cabling is poorly organized, not labelled and cannot facilitate adequate network troubleshooting which could lead to increased server downtime. There is also a lack of appropriate Uninterruptible Power Supply (UPS) devices in place to enable a controlled server shutdown in the event of a power failure as well to control power surges.

Inspection of the security permission on the database indicated that the "DELETE" function is not allowed on the EPICOR databases in critical database tables where transactions have been posted preventing the deletion of transactions in these tables.

We also found the following in relation to user rights and access

- Access is granted based on an approved user access form. A user is first required to be granted access to the Citrix Active Directory and then the Epicor Systems Administrator proceeds to grant access to the required and approved Epicor functions. A user is granted access to Ministry databases at two stages, first at the Citrix access setup stage and then at the Epicor application level. Should a user be granted access to for example Ministry A and B via Citrix and they are then granted access to Ministry A,B,C via Epicor once logged into the Citrix Desktop they will have access to the Epicor application and IFMIS reports and will be able to access all three Ministries.
- Comparison of user access rights for June 2014 indicated that users have access to more than one ministry within EPICOR.
- The Epicor System Administrator with username "SA" should only have enquiry (read only) access however analysis of his access rights indicated that he has modify rights within certain ministries.
- There is currently no periodic user access review performed to identify users with incorrect access rights. It was noted that the current IT Consultant prepares a monthly user access rights list for the Accountant General, IT Directors and IFMIS Manager however this list is not reviewed and nor is it utilised to facilitate effective control by performed a user access review.

- User access is currently not restricted to the user's individual terminals, allowing users to log into other users' computers with their own login credentials.
- IT is not notified by human resources of terminated users who longer work for the government of Malawi. As a result terminated users are not removed from the Active Directory as well as EPICOR.
- Audit Logging on the Active Directory for user account management is not enabled. Thus an audit trail of when users are granted access, when access is disabled is not logged.

We also found that the anti-virus database is updated once a week manually and not automatically updated as it has not internet connection to update the virus database. Finally we noted that the current version of EPICOR (7.3.5 which is approximately 10 years old) does not have the functionality to automatically disable suppliers after a prescribed period of inactivity. Suppliers need to be manually flagged as inactive. This will require continual monitoring.

25. Acknowledgement

We would like to extend our thanks to the many people who have assisted us with our work, in particular staff at the commercial banks, several of whom assisted the team outside of their normal duties to ensure that the necessary evidence has been made available

Report Ends