Donors and Implementing Partners fraud survey in Zambia

December 2019

pwc

www.pwc.com/zm

Contents

1 Foreword

Charity Mulenga

We are delighted to present the findings of our inaugural Donors and Implementing Partners (IPs) Fraud Survey in Zambia. The report is the culmination of several interactions with stakeholders as well as research into issues that affect the sector.

Funding from Donors has an important role to play in Zambia's economy as it contributes to and enables the implementation of the Government's social policies. The sector is not immune to social challenges which could impact achieving the United Nations Sustainable Development Goals (SDGs) in Zambia. Incidences of fraud in the sector serve to divert resources that are meant to be used to help achieve SDGs which include SGD 2: Zero hunger, SDG 3: Good health and well being, SDG 4: Quality education and SDG 16: Peace, justice and strong institutions. These challenges have become more critical as the Government considers how best to achieve economic and social development.

Donor funding is coming under increasing pressure due to economic challenges around the globe. The resources in developing countries and the demand for greater accountability of scarce resources means increased competition for Donor support.

Because of the unique challenges, we focused our survey on this segment of the sector to address fraud challenges faced by Donors and IPs. If fraud is not prevented and controlled it can erode confidence, leading to a reduction in funding from Donors and affecting social development.

At PwC, our purpose is to build trust in society and solve important problems. We believe that this report provides valuable insights into the state of risk of fraud among the Donors and IPs and we hope it will inform industry decision-makers and society members at large as they deliberate on ways to manage the risk of fraud. Additionally, we have included an article on *'Digitisation of Financial Services between Government and Citizens in Zambia'* from an industry expert which articulates the strides made by Government and challenges that are faced to fully adopt the use of digital plartforms. As Donors are investing in the social sectors of Government, the interventions that are being implemented should be of interest to them since these would assist to better managing resources allocated to the sector.

We are grateful to all the Donors and IPs who gave their valuable time to contribute to this survey. We hope that the findings make for interesting and useful reading.

Charity Mulenga
Partner
Government and Public Sector Leader
PwC Zambia

2 Executive summary

63%
of respondents are from executive management.

The PwC's inaugural Donors and Implementing Partners survey focused on the prevalence of fraud in Zambia.

The survey was conducted between 1 October 2019 and 21 October 2019 and consisted of a questionnaire that was sent out to Donors and Implementing Partners ('IPs').

In total, 42 questionnaires were sent to Donors and 73 to IPs. 23 Donors (54%) and 27 (37%) IPs responded. The composition of respondents included 63% from executive management, 20% middle management and 17% junior level staff. The PwC approach requires a minimum of 50 responses to generate a survey report, which this survey has achieved. The survey sample included International Donors and IPs.

The survey identified procurement and misappropriation of cash as the main areas where fraud arises. The survey also analysed how fraud incidents were discovered, who the typical perpetrators of fraud are, what actions are being taken when fraud is discovered and risk mitigation measures undertaken to manage fraud risk.

The survey asked respondents to report on the incidents of fraud within their organisations. About 48% of respondents stated that they had reported procurement fraud and 8% of respondents reported cases of misappropriation of cash. The respondents categorised Health, Education and Advocacy as the sectors most prone to fraud. The analysis of the survey also indicated that kickbacks from suppliers are the most prominent source of procurement fraud (at 43%), with the least being payment of personal expenses from donor funds (5%). Misappropriation of cash was another area where fraud incidents were reported. The survey results indicated that 33% of IPs who moved cash to remote places identified incidents of misappropriation of cash. One specific type of misappropriation of cash reported by the Donor respondents was theft and skimming.

Movement of cash by IPs to recipients in remote places was reported to be physically delivered by about 24% of respondents. Of these, 16% did not have cash-in-transit insurance and security. It is expected that the incidence of cash fraud would be high among organisations that handle significant amounts of cash, as handling physical cash increases the opportunity for fraud.

Incidents of fraud were reported to have occurred among the respondents that had weak internal control processes. Management override of controls was ranked highest among the respondents as being one of the key contributors to fraud incidents occurring. This happens when people in a position of authority circumvent the internal controls for their own personal benefit. The respondents reported that the lack of management review and internal controls could be indicative of a poor organisational culture or the non-existence of processes which are aimed at mitigating these incidents of fraud. The lack of independent checks and audits were also noted to be among the ways in which fraud arose.

About 64% of respondents who had experienced fraud stated that the perpetrators of their fraud incidents were junior staff, which is in line with the Association of Certified Fraud Examiners *2018 Report to the Nations ('ACFE')*, which also highlighted that junior staff were the highest number of perpetrators. The remaining 36% of cases were reported at more senior levels, of which 9% was reported to be committed at Board level.

We noted from the survey that there are a number of schemes that organisations employ to try to detect any potential risk of fraud. From the surveyed respondents, about 56% of those that had uncovered the fraud did so through internal and external audit channels, while the rest were split between whistleblowing and verification during surprise visits.

With regard to the surveyed IPs, 48% of them reported the incidents of fraud to the Donors. Of the surveyed Donors, 35% responded that they had received reports of incidents of fraud from the IPs. The variation in the results could be driven by the fact that some IPs have Donors that are based outside Zambia and were not part of our population. The IPs further indicated that where they had not reported the matter to the Donor, disciplinary action was taken against the perpetrators, which included dismissal, recovery of funds and reporting to the law enforcement agencies.

Pre-award assessments were highlighted as some of the interventions that both Donors and IPs use in assessing the robustness of the internal control frameworks of the recipients. While 72% of IPs underwent pre-award assessments from Donors before funds were disbursed, 39% of the IPs indicated that Donors altered funding following the gravity of the issues highlighted in the pre-award assessments.

Good corporate governance continues to be embraced among the surveyed population, as evidenced by the responses received. All the respondents indicated that they had a Board in place. However, over 50% of these respondents stated that internal audit functions continue to be an effective way of monitoring compliance and assisting in fraud detection. The Board of Directors are required to set the right tone at the top in order to ensure that controls are properly implemented and adhered to.

The respondents highlighted the use of computerised procurement and monitoring and evaluation systems, mobile payment platforms and financial management systems as areas that are increasingly being utilised by IPs in order to increase efficiency and manage the risk of fraud. Procurement process was reported among respondents (48%) to lack automation – and as a result the prevalence of fraud in this area was on the higher end. Mobile payment on the other hand indicates that there is an increase in uptake for organisations that make bulk payments. However, the users have not been alerted to the risks that arise from using this technology.

In summary, fraud continues to be a significant challenge faced by both Donors and IPs. The continued prevalence of fraud could have serious consequences with regard to the confidence levels within the sector, thereby affecting the delivery of the social services which most IPs and Donors provide on behalf of the Government.

It is therefore imperative that the respondents effectively implement fraud mitigation measures such as:

- Pre-award assessment by Donors before awarding funds to IPs;
- Embedding good corporate governance principles;
- Inculcating a whistleblowing culture;
- Performance of internal and external audits; and
- Use of technology.

3 Survey findings

Methodology

Who contributed to our survey?

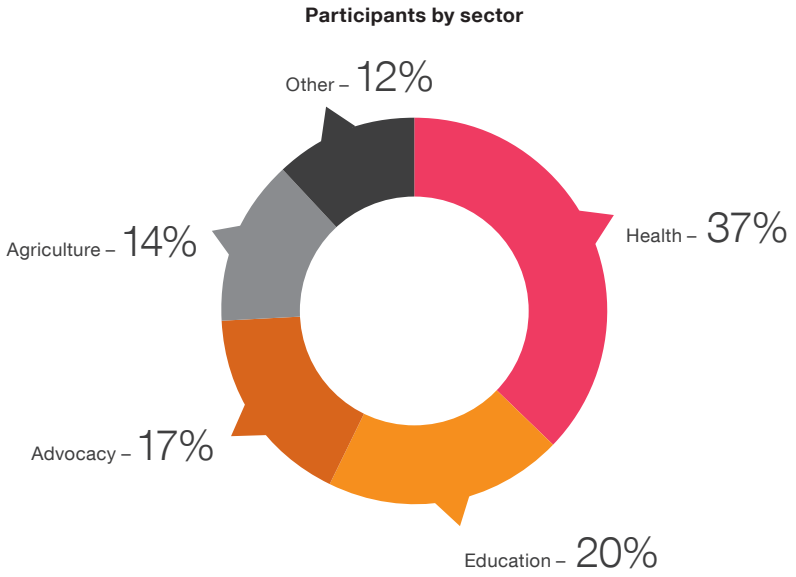
As a preamble to the survey, the team conducted interviews with selected stakeholders, and the results informed the need for the survey together with the structure of the questionnaire. This was circulated to Donors and IPs that agreed to participate.

The questionnaire was interactive and allowed respondents to provide responses based on whether they were a Donor or an IP. It was circulated to both management and non-management staff of the selected organisations. The areas that informed the survey questions are outlined below:

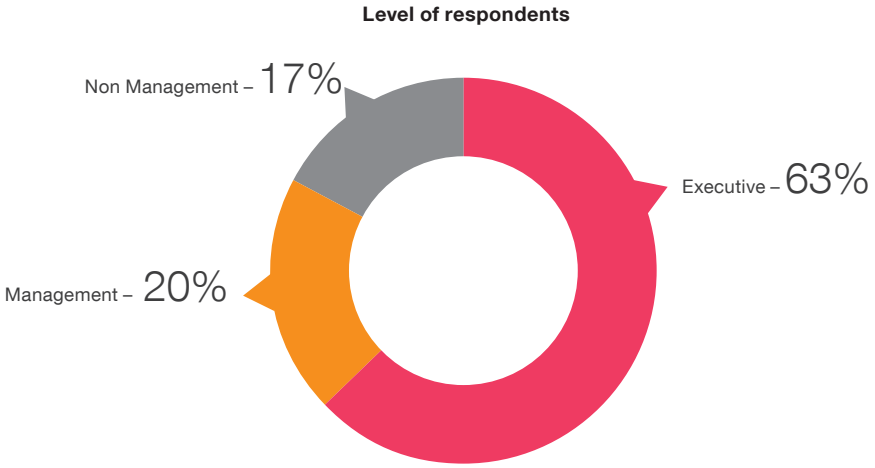
1. Risks in procurement, cash management and sub-grantee management, focusing on fraud incidents, actions taken and perpetrators; and

2. Fraud mitigation mechanisms around pre-award assessments, corporate governance, whistleblowing, internal and external audit and technology utilisation.

We asked our participants to select which sector they support. The sectors are featured in the graph below:



Respondents were also requested to provide details about their position so as to add context when conducting the initial analysis. The breakdown of the employee level of the respondents is as below:



Analysis methodology

The team further collated the responses and conducted a data-cleansing exercise to ensure that only questionnaires that were completed were included in the analysis.

Findings were compared against the *PwC 2018 Global Economic Crime Survey ('GECS') and ACFE 2018 Report to the Nations* to analyse the results from the respondents for similarity and comparison.

In calculating the percentages discussed throughout this report, we used the total number of complete and relevant responses for the question(s) being analysed.

In addition, we supplemented the survey findings with interviews from respondents to ensure that we obtained a full understanding of the answers provided.

In analysing the survey results, we have split responses between Donors and Implementing partners in some sections.

4 Risk profile by sector

The respondents were asked how they rated the risk of fraud in the sector they support, and these were their responses.

Risk profile by sector

Category	Health	Education	Advocacy	Agriculture	Other
Profile	⚠	⚠	⚠	⚠	⚠

⚠ Medium to high risk ⚠ Low to medium risk

According to selected respondents, the criteria that influenced their responses were strength of internal controls and tone at the top, the nature of activities they support, such as the number of sub-recipients they oversee, and those that implement community activities which are prone to fraud because they largely involve the use of huge amounts of cash for distribution.

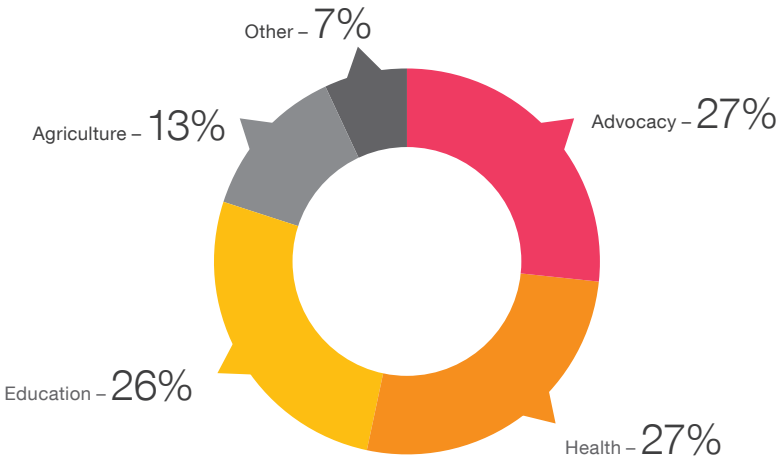
Further, the majority of the respondents believe that sectors with significant monetary Donor investments, especially those relating to basic necessities (e.g. Health, Education and Agriculture) are more prone to risk of fraud.

In the Health and Education sectors, the risk of fraud was assessed as medium to high risk due to the significant amount of grant refunds that have been requested by Donors from the Government institutions serving as IPs. The refunds are largely triggered by breach of grant agreements/funding requirements, especially cases of unsupported and unauthorised expenditure. The Donors also base their assessment on reports issued by the Office of the Auditor General.

5 Fraud incidents

We asked respondents to indicate areas where most fraud incidents occurred, and 56% of them reported incidents in the last 12 months. 48% of respondents stated that they had reported procurement fraud and 8% of respondents reported cases of misappropriation of cash. The respondents categorised Health, Education and Advocacy as the sectors most prone to fraud.

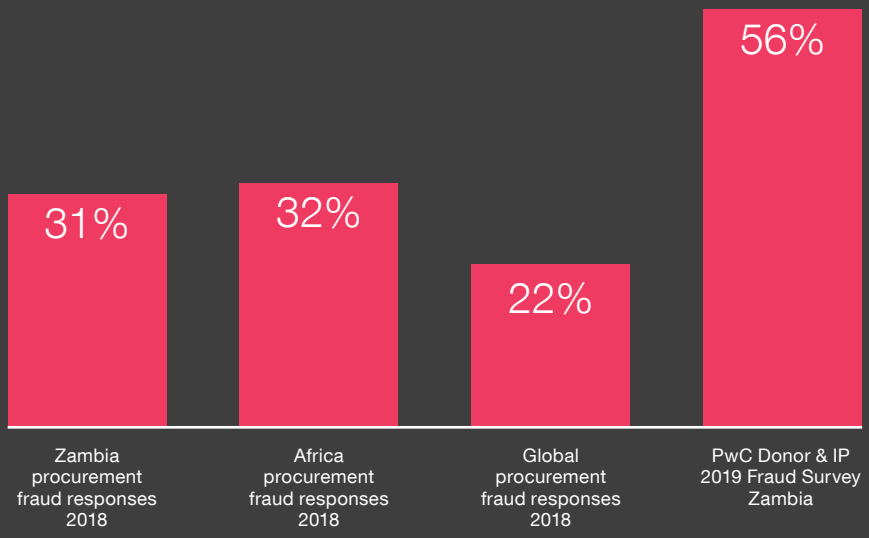
Fraud incidence by sector



Procurement fraud

Overall, 56% of IPs confirmed that they had experienced an incidence of fraud in their organisations. According to the *PwC 2018 GECS Zambia* report, respondents reported a prevalence rate of procurement fraud of 31%, which is 9% higher than the global average of 22%, and slightly lower than the African incidence rate of 32%.

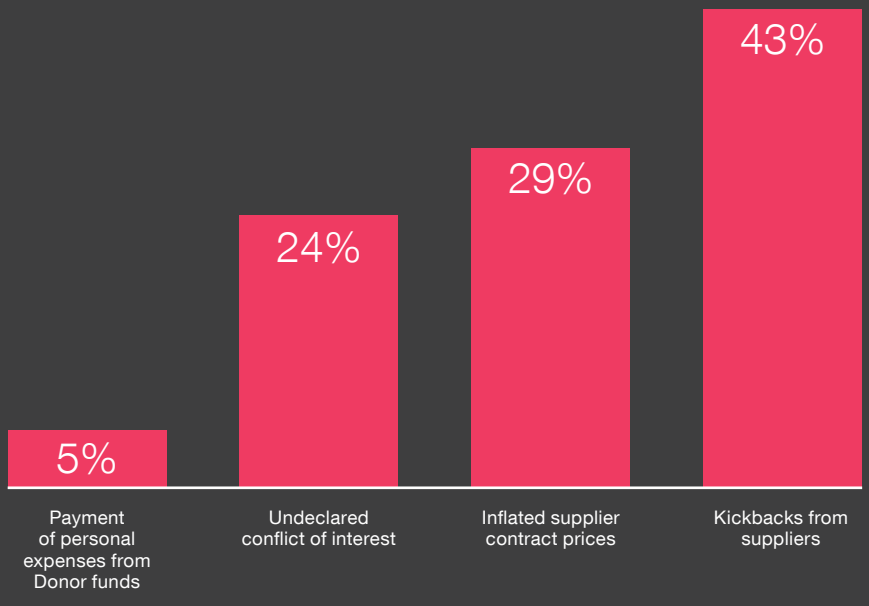
Fraud incidence by sector



The *PwC 2018 GECS Zambia* report included various other sectors such as public trading companies, private companies, Government/State-owned enterprises and NGOs, and this could therefore explain the difference in the prevalence rate of 56% in this survey against the 31%.

A further analysis of the survey responses shows that kickbacks from suppliers is the most prominent source of procurement fraud (43%), with the least being payment of personal expenses from donor funds (5%). We also noticed that the health sector recorded the greatest number of procurement fraud incidents (31%).

Types of procurement fraud



Procurement fraud involves abrogating the laid-down procurement rules and processes in engaging suppliers/vendors for goods and services with the intention of benefiting from the procurement activity. Procurement fraud can occur at any point in the process from needs identification to payment. Some of the examples in which procurement fraud can be perpetuated is through fixing prices, bid rigging, single sourcing, and payments for goods and services that were not received or were of poor quality.

The implementation of well-documented procurement guidelines and policies that clearly state the repercussions of procurement fraud is vital in preventing the occurrence of this type of fraud. In addition, the organisation's Board and senior management has to ensure that any suspected procurement fraud is investigated to its logical conclusion. All IP respondents stated that they had procurement policies in place, which is expected as it is a prerequisite from Donors prior to the awarding of grants.

Another control that counters fraud is the implementation of a computerised procurement system that has embedded control measures such as access controls, segregation of duties and approval limits. The survey results showed that 37% of IPs used computerised procurement process with embedded access controls and segregation of duties, while the remaining 63% used manual procurement systems.

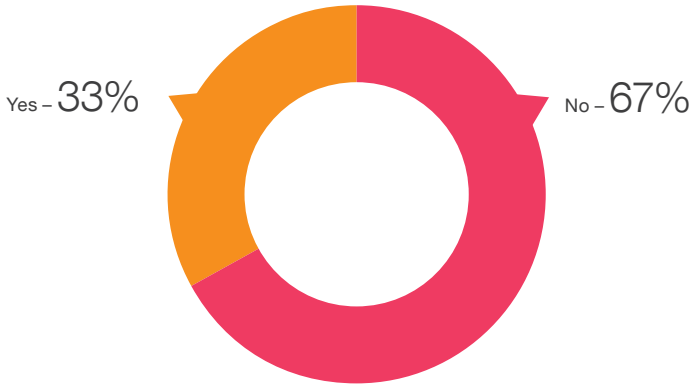
Misappropriation of cash

The ACFE defines asset misappropriation schemes to include both the theft of an organisation's assets, such as cash, and the misuse and theft of an organisation's assets, such as using an entity's car for a personal trip. This section discusses cash schemes that were reported from the survey respondents.

The survey results indicated that 33% of IPs who moved cash to remote places identified incidents of misappropriation of cash. This was due to the fact that the handling of cash increased the opportunity of fraud and therefore requires close monitoring of internal controls.

33%
of IPs who moved cash to remote places identified incidents of misappropriation of cash.

Fraud incidence with cash



One specific type of misappropriation of cash reported by the Donor respondents was theft and skimming. This is also known as 'off-book' fraud, which is the theft of cash from an organisation before it is recorded into any records or an accounting system. This mostly takes place in situations where cash is transacted without receipts being issued to a customer. It is one of the most difficult types of fraud to detect due to the lack of an audit trail that can be traced to the point of origin.

Regarding cash disbursements, the survey findings indicated that all respondents had a financial management system in place and therefore had basic internal controls to monitor the flow of cash and manage their expenses.

About 24% of respondents stated that they physically move cash to remote places. It is expected that the incidence of cash fraud would be high among organisations that handle significant amounts of cash. Organisations have the opportunity to reduce cash handling by working with financial institutions and mobile network operators to adopt secure methods of moving cash to recipients. Furthermore, 16% of respondents do not have cash-in-transit insurance and security. To manage this risk, best practice is to make use of the cash-in-transit services of security companies where cost effective.

Moreover, about 20% of IPs said they had experienced incidents of fraud at their sub-grantees. This would imply that assessments of the sub-grantees by IPs should be conducted before disbursing funds.

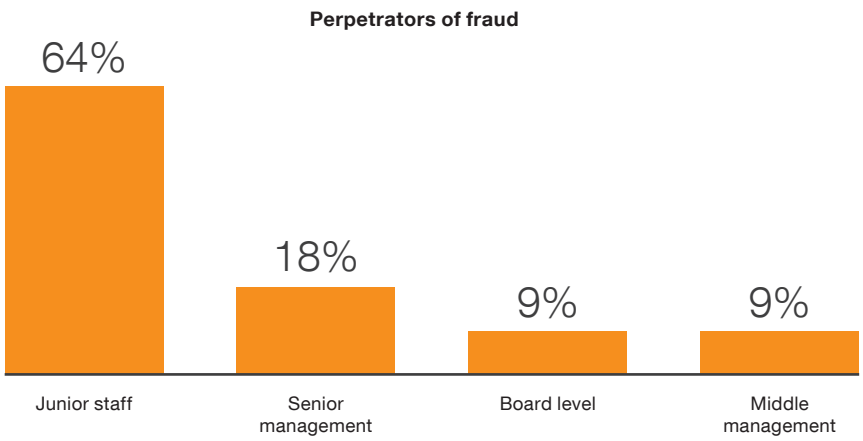
What led to incidents happening?

Typically, incidents of fraud are likely to occur where there are weak internal control processes. As part of the survey, we asked respondents to rank the internal control weaknesses that contributed most to fraud, with 1 being the highest contributor. Their responses were as indicated below:

Cause of risks	Rank
Management override of existing controls	1
Lack of management review	2
Lack of internal controls	3
Lack of independent checks/audits	4
Poor tone at the top	5
Lack of competent personnel in oversight roles	6
Lack of clear lines of authority	7

Management override of controls is a significant fraud risk in that people in positions of authority can perpetrate fraud by circumventing existing controls for personal interest/benefit. It is critical that there is adequate oversight to manage this risk. Lack of management review and internal controls could be indicative of poor organisational culture, or the non-existence of processes which are aimed at mitigating these incidents of fraud. A poor tone at the top could be driven by poor adherence to good corporate governance principles.

Perpetrators of fraud



About 64% of respondents who had experienced fraud stated that the perpetrators of the fraud incidents were junior staff, which is in line with the *ACFE 2018 Report*, which also stated that junior staff were the largest perpetrators of fraud. The *ACFE 2018 Report* further goes on to analyse the correlation between loss caused due to fraud and the perpetrator's level of authority, which was that the value of the losses is higher when the fraud is undertaken by someone who has a higher level of authority. This is due to employees at higher levels having greater access to an organisation's assets and being in a much better position to conceal fraud than those at lower levels in the hierarchy.

The remainder of the cases that were reported by the respondents at more senior levels are a cause for concern, especially given that 9% of these cases represented fraud committed at Board level. The Board of Directors is required to set the right tone at the top in order to ensure that controls are properly implemented and adhered to.

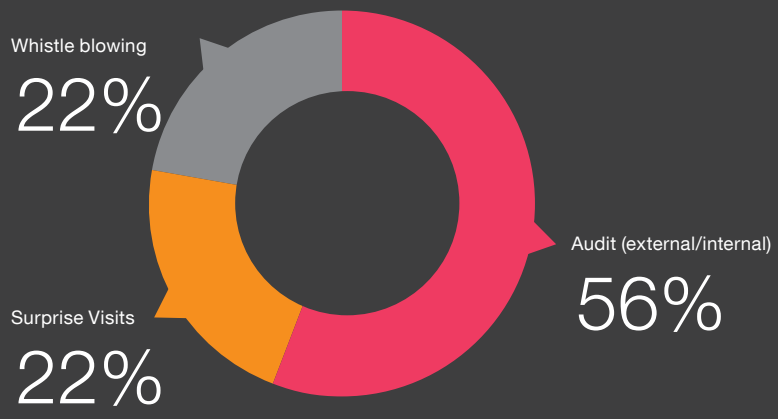
Where the Board is not sufficiently competent, fraud will likely not be detected or prevented. The independence of the Board also gives greater confidence to stakeholders that issues of fraud perpetrated by the Board will not thrive in the organisation. This is because the Board will self-regulate through the Board charter and the individual skills of each board member to critique information presented to the members to curb any fraud.

Discovery of fraud and actions taken

Organisations employ a number of schemes to try to detect any potential threat of fraud. About 56% of the surveyed respondents who uncovered the fraud did so through internal and external audit channels and the rest were split whistleblowing and surprise visits.

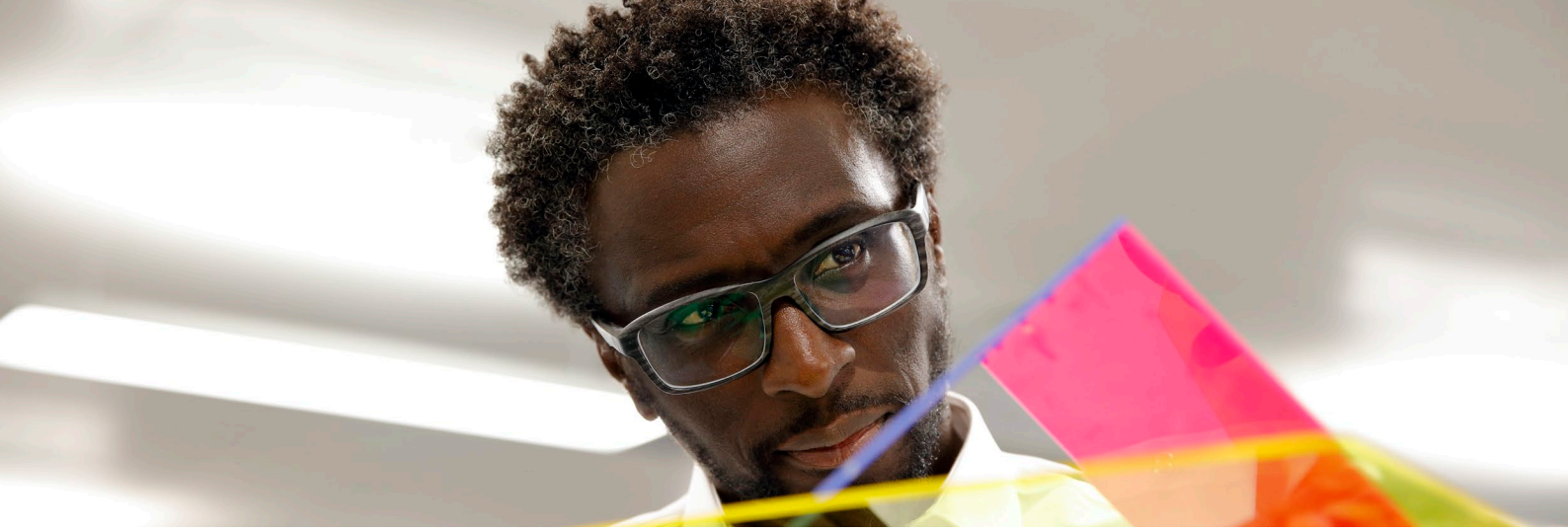
For whistleblowing to work effectively, there has to be a properly defined process which promotes and ensures anonymity to informers. All reported cases through this process will have to be investigated, but there is a need to ensure that before any case is prosecuted, proper evidence is gathered.

Sources of Fraud Discovery



The analysis around action taken indicates that the majority of the IPs (57%) had reported the incidents of fraud to the Donors.

The IPs further indicated that where they had not reported the matter to the Donor, disciplinary action was taken against the perpetrators. The disciplinary action taken included dismissal, reporting to the law enforcement agencies and recovery of funds misappropriated by the culprits.



6 Fraud risk management measures at Donors and IPs

Many organisations spend a great deal of time focusing on ways to prevent fraud before it occurs. Of the three sides of the fraud triangle – pressure, opportunity, and rationalisation – a lot effort has gone into addressing the opportunity to commit fraud, primarily through internal controls. Still, because fraud is the result of the intersection of human choices with system failures, it's important to be wary of the false sense of security that internal controls, even well-designed ones, can bring. Collusion, and the ability of management to override controls, means that no system can fully prevent fraud.

The Board and executive management need to understand the attributes of the fraud triangle as a way of understanding fraud red flags and why fraud is perpetrated in the first instance.

The fraud triangle is a framework designed to explain the reasoning behind why employees commit fraud.

'*Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property.*'[1]

Fraud mitigation measures are an important element of preventing and detecting fraud. We noted that the survey respondents have identified risk mitigation measures which they are implementing to prevent fraud. These include:

- Pre-award assessment by Donors before awarding funds to IPs
- Embedding good corporate governance principles
- Inculcating a whistleblowing culture
- Performance of internal and external audits; and
- Use of technology.

1. Donald R. Cressey, Other People's Money (Montclair: Patterson Smith, 1973) p. 30.

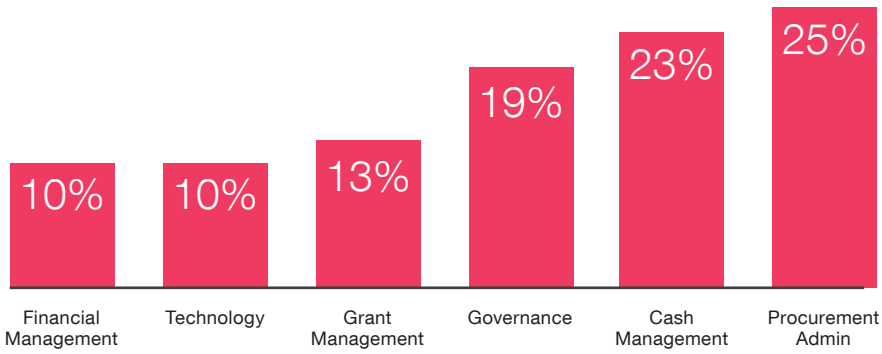
Below we indicate the current state of implementation of fraud mitigation measures from respondents and areas of improvement.

a. Pre-award assessments

Pre-award assessments are designed to give some assurance to funders that the IPs have the capacity to meet the requirements of the grant agreements.

The survey showed that 91% of Donor respondents stated that they undertake pre-award assessments prior to disbursement of funds. Lack of established controls and processes around cash management, financial management, procurement and contract management were the main issues Donors recommended IPs implement post assessment. This is consistent with responses from IPs who indicated that they implemented these controls. Donors also identified a lack of proper governance structures and non-qualified Boards at IPs as an issue of concern.

Controls implemented after pre-award assessment



Of the 91% of Donor respondents that undertook pre-award assessments, 65% said they altered their mode of funding after they received the results of these assessments. Donors altered their mode of payment by either withholding funding or reducing the funds disbursed until mitigating measures were implemented.

While other Donors may have various reasons for proceeding to fund despite the gaps noted at pre-award stage, it is important to note that many of the fraud cases which later occur tend to arise from the gaps identified during pre-award assessment. Significant weaknesses identified during pre-award assessments should be addressed by IPs before Donors disburse further funding. Weaknesses in the Boards is a significant area such that Donors should critique the Board composition and structure, skills level and experience. For further information refer to the corporate governance section of the report.

b. Embedding good corporate governance principles

An effectively well-run and controlled organisation promotes confidence in its stakeholders. Governance process involves the designing of tools (internal controls) to enable those charged with governance to execute their oversight roles in the organisation. Often, the tools designed, which are handed down to management for implementation, serve as the backbone and channel of the directives issued by those charged with governance to the management of the organisation.

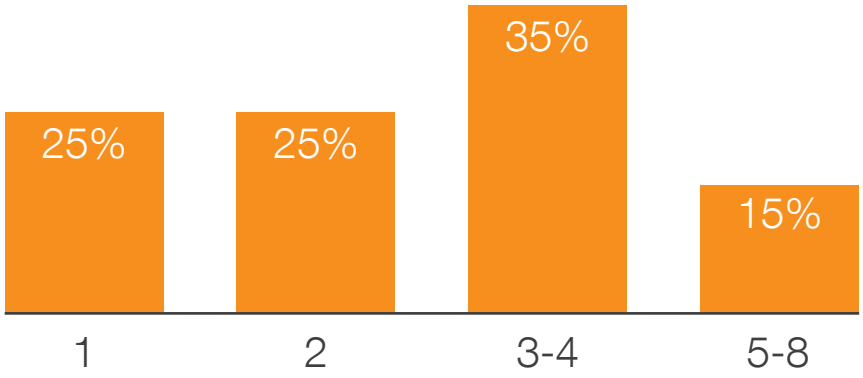
Good corporate governance practices recommend that an entity should have a well-balanced (skills, industry experience, independence and ethical standing), effective Board that meets regularly.

As part of its duties the Board is required to provide oversight and direction to management. This is done through regular meetings to discuss the strategic and operational performance of the organisation as per information provided by executive management.

The effectiveness of the Board in the prevention or detection of fraud lies in the sufficiency of the right blend of skills across the Board members to critique information coming from management as well as internal audit. This is because information from management and internal audit constitutes the bottom-up feedback mechanism which enables the Board to give tailored directives to ensure that fraud at the least does not occur, or, if it does, to contain the extent of its impact on the reputation of the organisation. In this regard, the Board members are required to be savvy with analysing and interpreting both financial and non-financial information before them. Some of the techniques include trend analysis, technical analysis, and keeping up with developments in non-financial areas such as ethics, sound Board practices, social practices and politics.

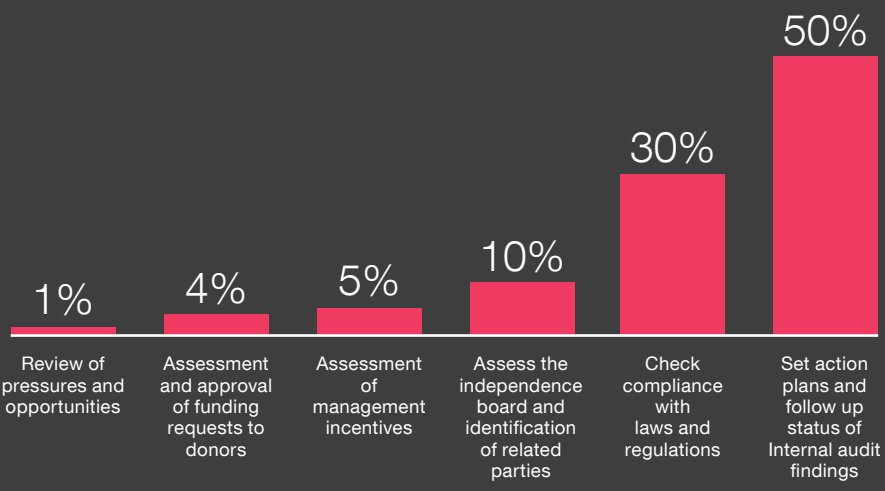
The survey results showed that only 15% of IP Boards met five to eight times during the past 12 months. The low number of Board meetings emphasises the concerns raised above, since Boards should meet at least four times in each financial year.

Number of meetings held



Respondents were asked to indicate the extent to which the Board assesses fraud risk. 50% said that the Boards relied on information presented by Internal Audit. The reliance on Internal Audit is a detection measure and a reactive approach to fraud prevention. Boards should focus on ensuring that proper systems of internal controls have been embedded into the organisation's operations.

Extent to which those charge with governance assess fraud risk



Typically, internal controls, openness and a strong organisational culture are the main attributes of a strong internal control environment. This then means that Boards of Directors need to ensure that:

- The organisation's internal controls (policies and systems) are robust and sufficient to prevent or detect fraud;
- Ethical conduct is promoted by establishing codes of conduct;
- Whistleblowing policies and hotlines are implemented;
- The lines of defence (control and compliance, risk management and internal audit) are enforced;
- A culture of openness about fraud is inculcated and clear reporting channels within the organisation are established; and
- A clear tone at the top is established and this is embedded in the entire organisation.

c. Inculcating a whistleblowing culture

An analysis of the respondents to our survey shows that employees were the top source of tips among the respondents. This is consistent with findings in the PwC 2018 GECS Zambia Report, which revealed that 54% of respondents in Zambia (compared to 52% in Kenya) stated that the review of whistleblowing reports was a key mechanism being employed to assess the effectiveness of compliance and business ethics programmes. The Association of Certified Fraud Examiners 2018 Global study on occupational fraud and abuse, *ACFE 2018 Report to the Nations*, also listed tips as the most common detection source of fraud at 40%.

Tipoffs as a whistleblowing mechanism

Cause of tipoffs	Rank
Employees	1
Vendors	2
Customers	3
Other Donors	4
Zambia Revenue Authority	5

Organisational leaders are increasingly realising that problems do occur – across all sectors. But if organisations create the appropriate culture, people will feel free to speak up when they suspect there has been a breach of ethics or values. Whistleblowing is just one part of the strategies to encourage this culture of transparency and open communication within organisations. In the past few years, the trend has been to rely on rules, policies, processes and controls in place, but we are now beginning to understand that it's also really around the culture and the transparency of how things are dealt with. While the onus is on the entire organisation to behave in an appropriate way, the message on transparency needs to come from the upper levels of management. Action from the top is absolutely critical if organisations are to encourage people to feel safe and secure in using the organisation's designated whistleblowing mechanisms. Where you have leaders who are genuine, who recognise and reward good behaviours as well as penalise poor behaviours, people trust them and believe there's authenticity and transparency around how challenging business decisions are handled.

Organisations should therefore encourage whistleblowing mechanisms by implementing the following:

- Gaining top-level commitment;
- Developing a whistleblowing policy;
- Designing whistleblowing reporting mechanisms;
- Embedding a whistleblowing programme; and
- Reporting, monitoring and evaluating the whistleblowing arrangements.

d. Performance of internal and external audits

The primary objective of an internal audit function is to provide an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. Internal audit helps an organisation accomplish its objectives through a systematic and disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.
On the other hand, external audits are limited to providing assurance on financial statements. External auditors focus on the financial transactions and controls related to financial reporting, while internal auditors cover the entire controls framework of the business, encompassing strategic risks, business risks, financial risks, operational risks, and legal, regulatory and reputational risks, among other things.

One similarity between internal and external audit is the concept of independence. It is crucial that an internal auditor not only be independent of the entity under review, but also report directly to the organisation's Board and Audit Committee.

It is good to note that 80% of IPs have internal audit functions. The remaining 20% indicated that they rely on embedded electronic control and soliciting guidance from the Board of Directors.

IPs need to ensure that they are getting value from their internal audit functions. The value derived could be achieved by IPs asking the following questions on internal audit functions:

- Does internal audit provide assurance on the organisation's governance, risk management, and control processes to help the organisation achieve its strategic, operational, financial, and compliance objectives?
- Is internal audit a catalyst for improving an organisation's effectiveness and efficiency by providing insight and recommendations based on analyses and assessments of data and business processes?
- In its commitment to integrity and accountability, does internal audit provide value to those charged with governance and senior management as an objective source of independent advice?

While external audits are typically commissioned by IPs for compliance purposes as per grant requirements from Donors, they play a crucial role in providing a fresh and independent perspective on the organisations' efforts to curb fraud.

Contemporary auditing standards such as International Standards on Auditing (ISAs) place the role of prevention or detection of fraud on the Board of Directors by implementation of a robust internal control environment. External auditors are however required to report fraud once suspected or detected in the course of their audit work. The inherent risk in the external audit is that the focus and indeed the procedures designed by the external auditor are for the sole purpose of giving the auditor grounds for issuing the audit opinion. In this fashion, the external audit may not detect fraud due to the limitation of the audit framework.

It is also important to note that while the role of an external auditor is clearly defined, auditors have on several occasions come under fire from the public jury where cases of massive frauds are unearthed. As a result, external auditors are alive to this unwritten expectation and ensure that they conduct thorough risk of fraud assessments as part of their detailed audit strategy. ISAs do require the auditor to evidence how they satisfied themselves that the risk of fraud is sufficiently assessed and reduced to tolerable levels in the context of the ISA framework.

Furthermore, the external auditor can revise the audit strategy at any point they suspect fraud during the audit and before signing off on the financial statements.

External auditors also issue a management letter which highlights the weaknesses in financial reporting controls as well as recommendations to address weaknesses uncovered during the audit period. There is a strong correlation between recommendations from auditors which are not implemented by management and the proliferation of fraud in the organisation. This then means that it is imperative for Internal Audit through the chain to the Board of Directors to also ensure that a clear traction of external audit recommendations is achieved by the time of the next external audit. It is therefore good practice that both IPs and Donors align issues identified from internal and external audit reviews and ensure that issues are clearly addressed.

The existence of internal audit, external audit and other assurance providers cannot substitute for having a robust system of internal controls. It is the responsibility of the Board and executive management to ensure that this is put in place and is implemented effectively.

e. Use of technology

Technological advancements are affecting how organisations are operating at every level. This can be seen in the increased integration of technology in day-to-day operations.

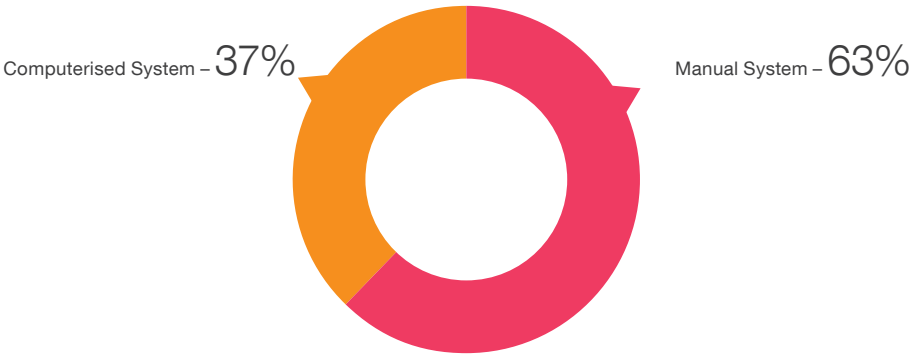
For organisations in the Donor space, the use of computerised procurement and monitoring and evaluation systems, mobile payment platforms and financial management systems are areas that are increasingly being used by both Donors and IPs in order to increase efficiency and manage the risk of fraud.

63% of respondents who had stated that they had incidents of procurement fraud indicated that they did not have computerised procurement systems. This indicates that using computerised procurement systems hinders fraud perpetrators in the following ways:

- They provide an audit trail which makes the internal audit reviews easier;
- Segregation of duties will be enhanced by embedded controls in the system and different access rights; and
- Better visibility into the procurement process.

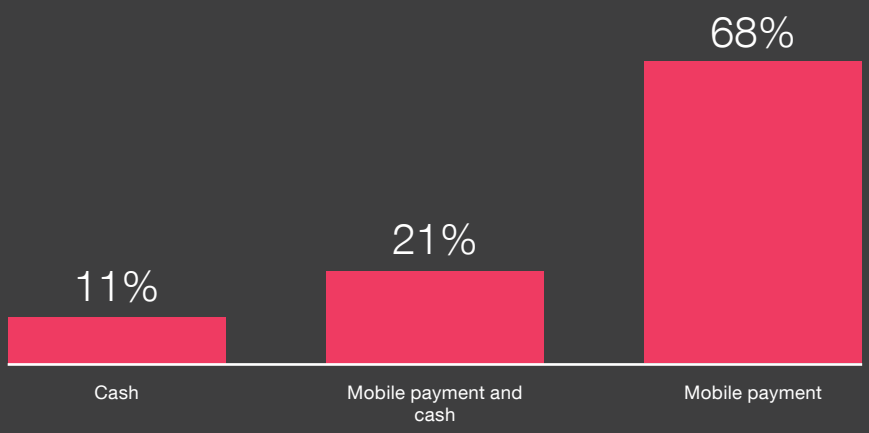
IPs are therefore encouraged to use computerised procurement systems as a means to deter fraud perpetrators.

Procurement fraud prevalence – computerised vs manual system



Mobile payment platforms are another use of technology that is becoming common. The survey findings also show that over 68% of IPs who make bulk payments used mobile payment platforms. The use of mobile payment platforms is likely to increase further, with the majority of respondents projecting that the proportion of payments made using mobile payment platforms will increase significantly in the next five years.

Payment Platforms used

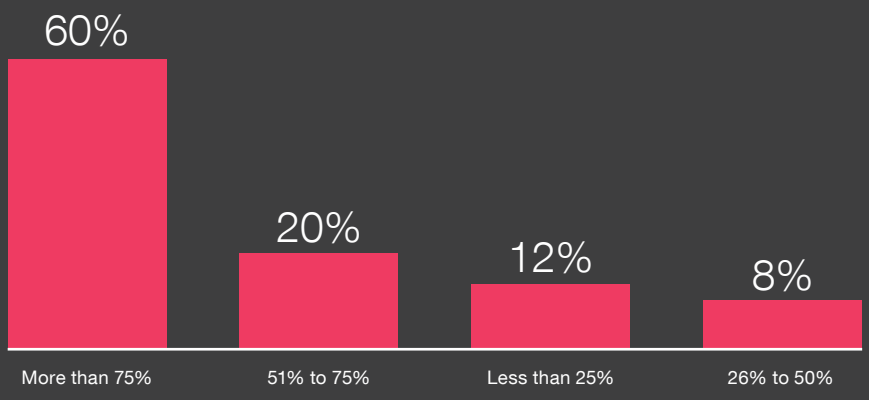


As use of mobile payment platforms become prevalent, organisations need to be alert to potential fraud red flags arising from the use of these systems.

Controls that should be included comprise:

- Reviewing the accuracy and completeness of data submitted for mobile payments;
- Performing regular reconciliations of data submitted for payment to the bank against payment reports received from the bank; and
- File protection using encryption software.

Projected use of mobile payment platform in 5 years



7 Conclusion

The survey has reiterated that procurement and cash misappropriation are the most common forms of frauds being committed. In response to the risk of fraud, Donors and IPs are implementing measures, including conducting pre-award assessment by Donors before awarding funds to IPs, embedding good corporate governance principles, inculcating a whistleblowing culture, performing internal and external audits and using technology. As highlighted in the report, collusion, and the ability of management to override controls, means that no system can fully prevent fraud. Management override of controls was the most significant root cause of why the fraud incidents reported were happening.

The report has identified areas to improve in order for the mitigating measures to be more effective. One area is enhancing the pre-award assessment process and ensuring that recommendations from the process are effected. We noted that most IPs had undergone pre-award assessment before grant signing and 25% of the controls that were implemented post award assessment related to procurement controls, yet the IPs had more procurement-related fraud incidents.

Another area for improvement is getting the most out of Boards. This should include ensuring members have the right skill sets, are independent, meet regularly and focus on ensuring that proper systems of internal controls have been embedded into the organisation's operations. Whistleblowing was the most common form of detecting fraud in the organisations surveyed, which confirms the need to increase levels of awareness of this channel. It requires a strong tone at the top and working at gaining the trust of employees that these processes work and yield significant benefits to the individual and to the organisation itself. Also, as highlighted in the report, most of the organisations surveyed have an internal audit function, and the function plays a significant role in preventing and detecting fraud. It is imperative that organisations ensure that they get the most value out of the function. Areas to consider are highlighted in the report.

The survey results have also shown an increased use of technological enhancements such as mobile payment platforms, automated financial management systems and procurement systems. However, the results show that use of manual systems in the procurement process is still very high and is linked to the occurrence of fraud. This therefore emphasises the need for IPs to embrace the use of technological applications that have minimum controls embedded in the system. With regard to misappropriations of cash, the survey indicated a lower incidence rate for organisations that had reduced cash handling by use of technology.

The progressive move to use more technology should be approached with caution by IPs and Donors alike, as emerging risks arising from new technological innovations might impede their efforts in fighting fraud. Adequate controls must be put in place beforehand.

8 Digitisation of financial services between Government and citizens in Zambia

Betty Wilkinson
Chief Executive Officer
FSD Zambia

Digitisation of financial services is often called an essential part of the Fourth Industrial Revolution of our world. Increasingly, the use of electronic communications devices and systems to both process financial transactions and to analyse the flows of funds is a reality around the globe. While there are a number of reasons why countries are moving to digital transactions with their citizens and others [1], the main ones listed are transparency, cost savings by governments, speed and security, financial inclusion, and economic development.

Digitisation will provide an important avenue for African economies to leapfrog not only financial development but also development across other sectors of the economy, including the one where Donors and IPs operate. There are infinite opportunities on the digital platform, and fintechs are working round-the-clock to develop and introduce new products here. However, these changes will benefit only those economies that embrace digitisation, invest in the required infrastructure, and introduce commensurate regulatory technology. Digitisation is transforming African economies in four major ways: retail payments systems, financial inclusion, sustainable business models, and revenue administration.

However, there are also challenges faced in moving in this direction. Research in 2017 stated that 'Most importantly, digitisation may require significant up-front investments in building an adequate physical payment infrastructure that is able to process such payments, as well as a financial identification system and a consumer protection and education framework to ensure that recipients have safe, reliable, and affordable access to the digital payment system.'

Zambia is committed to and is undertaking early stage development of government digitisation of payments to help ensure financial inclusion and to address the multiple challenges of a very cash-heavy economy. The Bank of Zambia has publicly committed to moving the financial sector and the economy at large from cash transactions to 'cash lite' by the expansion of digital financial services. The creation of the SMART Zambia Institute ('SZI') in the Office of the President in 2016 has established a formal home to coordinate and implement e-government for improved service delivery. This has included Treasury authority and setup of SZI, to grow digitisation of government payments – particularly bulk payments. Currently there are citizen e-services for payment of taxes to ZRA, registration of businesses through PACRA, civil servant pay, and payment of contributions to certain subsidies such as the Farmer Input Supply Programme. There have been significant investments in

hardware and software to engage in the development of such services, both financial and informational, across the country in the last two years. Work to consider how to translate the near-universal movements of cash throughout Zambia to bulk payment by mobile money agents or other financial institutions is also under way.

There are developments in process to encourage foundational digital identities for all citizens and residents, which can significantly enhance the process of digital payments of all kinds. There are new systems being tested to digitise the payments of social security (also called social cash transfers) for the poorest households. This includes opportunities for eligible citizens to participate more fully in programmes such as the GEWEL project of the World Bank to sustainably improve incomes for some of the poorest women in Zambia.

So, if this is a good idea, what are the limitations to digital financial services provision and related digitisation processes by government? They come down to three: infrastructure, government installation costs, and popular culture around money.

The most crucial challenge is **infrastructure**. To make government e-payments a reality both to and from citizens, there needs to be reliable supplies of electricity and cell phone communications to and from citizens and businesses. With the current circumstances of power outages due to lack of water in hydropower systems, true availability is below the 2017 data showing 40.3 percent of households had electricity[1]. While undoubtedly solar systems are rapidly changing these numbers, it still means that over half the population will be unable to charge a basic cell phone to access e-financial services. Serving cell phones also requires towers. In this area much has improved, and the significant expansion of towers over the last two years is pushing services to the anticipated 98% of populated areas in the next year or so. The difficulty will be in quality of signal, as currently a third of clients are complaining about poor signal quality, and this will not encourage the use of cell phones for mobile money services use and expansion. A key end point is that people need cell phones, and in Zambia the numbers of those who own handsets is still very low, especially women. The entry point of digitisation has been through the telecommunications sector, given the diverse products available on the mobile phone and its replication capability across countries.

The second challenge is the **government installation costs**. These exist in three forms. The first is an evaluation and revision of rules, in the form of legislation, regulation, and government processes. After this, digitisation processes have to be examined and established to ensure an effective transition. This means defining and implementing methods to enable the changeover, from digitisation of forms and requests to processing of payments to and from citizens with meaningful access. This might mean government civil servant retraining and may even mean staff changes. And if a consumer cannot receive funds because there are no mobile money agents nearby, he or she will have to travel long distances at high cost and may reject the process. Third, there are the investment costs of such a change. Payments to and from government will require public-private engagement and significant investment to make sure the systems are enabled.

The third challenge is **public attitudes**, and these are very difficult to shift. Zambians are generally considered to be slow adapters to new technology because it has proven very unreliable to access, and to easily and consistently use. While there has been expansive growth in general use of mobile money services, as shown both in the UNCDF State of the Digital Financial Services Market in Zambia 2018 report and the ZICTA 2018 National Survey on Access and Usage of ICT, the types of services used are restricted. Most clients – and they are largely male – use digital financial services to send and receive money to family and friends. This means that they are using the services to shift cash value. It is paid to an agent and received and immediately translated into cash on the receiving end. Thus, the ongoing problems for clients are mobile money agent liquidity, ability to use noncash to shift to and from mobile wallets to pay for goods and services, and reliable cell phone signal. Without resolution of these challenges, public acceptance of digital financial services generally will remain low and willingness to engage in government transactions will equally be limited.

It is important to realise that people want to know what the true position of a given payment is at all times. With cash, you can understand where the money is: it is in your hands or the government's hands, as there is cash and receipts which are both physical. With e-transactions there may be text messages involved, but it is not yet considered by either party to be acceptable proof of payment. Thus, we need mechanisms to provide unequivocal methods for the proof of payment – whether a credit to an account or mobile money wallet, or a recognition of the transaction generated by a key government agency such as SZI. In this way, if there are any problems later, the citizen can use the notification to clear up issues.

Finally, it will be quite important in Zambia to address the costs of the transactions. Currently there are no extra fees for government to pay or receive cash for the citizen. However, there are significant transactions costs for mobile money or e-payments. Ideas for addressing this might include reducing the taxation on phone usage for e-money and related cell use transactions; or government compensating citizens for e-payment of other electronic transactions fees from mobile money providers when payments to government are made. If the systems are reliable and proof of payment is strong, then customers may be willing to pay for the convenience of such transfers.

The challenges above may seem daunting, but good progress is being made. The biggest challenge – a commitment to move forward with this process – has already been met. The next one – infrastructure – is being worked on and is improving with time. Analysis of what it will take to enable e-financial transactions to be more common and more effective is under way. The importance of talking to and educating citizens and ensuring that the processes of e-payments to and from them and the government are effective is the next fundamental work area. Zambians everywhere are intelligent and respond well and rapidly to services which are simple, affordable, and easy to understand and use. If they resist it is a matter of both usability and trust. This is the next and most significant challenge and yet it can be met – look at how fast digital financial transactions are growing!

9 Our Comprehensive Forensic Solutions

PwC offers end-to-end active anti-corruption, fraud prevention and investigation solutions to help clients assess fraud; design, implement and maintain a fraud prevention strategy; and to develop incident response mechanisms. Our forensics and dispute analysis professionals can assist your organisation by providing a wide variety of advisory services and investigations including:

Fraud prevention and anti corruption services

- Fraud risk assessments
- Fraud health checks
- Fraud detection reviews
- Fraud and corruption risk management strategies
- Whistleblowing
- Capacity building in fraud prevention

Investigations

- Fraud investigations
- Expert witn ess services
- Litigation support services
- Bribery and corruption
- Asset tracing and recovery

Regulatory compliance reviews

- Compliance with Anti-Money Laundering regulations
- Compliance with the US Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act
- Compliance with other regulations

Forensic technology solutions

- Imaging of electronic media
- Data recovery
- Acquiring and analysing computer files
- Cyber crime prevention and response

Corporate Intelligence

- Provision of objective, clear and targeted investigative research and analysis
- Better understanding of acquisition targets or business partners e.g. customers, suppliers, agents, licensees
- Intelligence to inform major strategic decisions

Dispute support services

- General commercial disputes
- Transaction related disputes
- Intellectual property disputes
- Competition/anti trust disputes
- Capital projects and infrastructure disputes

10 Contacts

Want to know more about what you can do in the fight against fraud?

Contact one of our forensics specialists:

Nasir Ali
Country Senior Partner, PwC Zambia
+260 (211) 334 000
nasir.y.x.ali@pwc.com

Charity Mulenga
Partner, PwC Zambia
+260 (211) 334 000
charity.mulenga@pwc.com

Muniu Thoithi
East Market Advisory Leader
+254 20 285 5684
muniu.thoithi@pwc.com

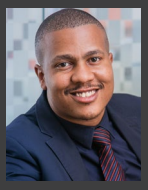
Moonga Hamukale
Senior Manager
+260 (211) 334 000
moonga.hamukale@pwc.com

Report Contributors

Charity Mulenga
Government & Public Sector Leader – PwC Zambia
charity.mulenga@pwc.com

Peter Kalala
Manager – Assurance
peter.kalala@pwc.com

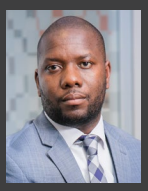
Moonga Hamukale
Senior Manager – Advisory
moonga.hamukale@pwc.com



Malama Mwilwa
Associate – Advisory
malama.mwilwa@pwc.com

John Sakala
Senior Manager – Assurance
john.s.sakala@pwc.com

Jacob Kalumba
Manager – Assurance
jacob.j.kalumba@pwc.com



Mwiya Mwiya
Senior Manager – Assurance
mwiya.mwiya@pwc.com

Evelyn Tembo
Senior Associate – Clients & Markets Development
evelyn.tembo@pwc.com

Betty Wilkinson
Guest contributor
Chief Executive Officer
Financial Sector Deepening Zambia

Kasongo Lufuma
Senior Associate – Clients & Markets Development
kasongo.lufuma@pwc.com

Leya Musonda
Senior Associate – Assurance
leya.musonda@pwc.com

www.pwc.com/zm

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

(19-24876)