Adjusting the Lens on Economic Crime in Zambia

Turning opportunity for crime into opportunity for growth

61%

report having experienced some form of economic crime

38%

of economic crimes detected through means beyond the influence of management

60%

of economic crimes committed by internal fraudsters were as a result of Opportunity/Ability to commit the crime

pwc

Contents

Foreword

Nasir Ali
Country Senior Partner
Zambia

Muniu Thoithi
Forensics Leader (East Market)
PwC Kenya

The last 24 months have been a testing time for Zambia. In addition to the sudden death of the former President, His Excellency Michael Sata in October 2014, the country has also struggled with falling copper prices, a depreciating currency and country-wide power shortages.

Zambia's gross domestic product (GDP) is expected to be significantly less than projected as a result of recent challenges, with projected growth being revised down from 7% to 3.5% (World Bank data) in 2015 – largely caused by the reduced copper output. Copper prices have fallen from an average of US$6,829 per tonne in 2014 to US$4,605, making it economically unviable for some Zambian mines to continue operating. Given that Zambia is heavily dependent on copper – accounting for 80% of export earnings – the reduced value of copper has acted as a catalyst for the country's economic woes.

Poor rainy seasons have also contributed to Zambia's economic challenges leading to nationwide power cuts which have affected productivity and ultimately reduced output across all sectors. The load shedding has also led to increased production costs as business owners seek alternative energy sources. While the Government is undertaking short-term measures to address the issue, such as importing power from abroad and introducing tax incentives to encourage private investment in the energy sector, Zambia's power woes continue to affect the economy as a whole.

The Kwacha was the world's worst performing currency in 2015, plummeting to half its value during the first eleven months of the year. In addition inflation increased from 7.9% to 21.8% between September 2015 and January 2016 (Central Statistics Office). This was as a result of both international and domestic factors including a strong US dollar, reduced supply of foreign exchange earnings from copper and relentless power issues.

The last 24 months have been extremely tough on not only local businesses but also the Zambian people. With the costs of everyday essentials almost doubling in price many are on the brink of financial despair – and desperate times call for desperate measures. The current state of the Zambian economy has created a playing field for those wishing to take advantage of weak internal controls for personal gain and thus allowing economic crime to thrive.

It was in this environment of turmoil that we conducted our 2016 Global Economic Crime Survey. This year's survey results reveal that the rate of economic crime in Zambia has increased by 36% since 2014- the largest increase reported from the 115 participating countries in 2016. Zambian respondents have reported the third highest rate of economic crime in the world (61% of respondents had suffered an incident of economic crime) and is among the top three in Africa. Types of fraud that have seen a significant increase over the last 24 months include accounting fraud and cybercrime which have affected organisations across a range of sectors. All organisations in the course of daily business face exposure to various types of economic crime from multiple angles as they interact with third parties to create or exchange value. With the Government warning that recent challenges will likely remain in 2016, the question arises – what are organisations doing about the increased threat of economic crime? Are they even aware of its escalation?

Our report challenges you to adjust the lens on economic crime and refocus your path towards the opportunities around strategic preparation. Understanding the vision of your company as well as planning for defence will be the difference between maximizing your opportunities or allowing those who want to victimize you to capitalize on theirs.

We would like to extend our sincere gratitude to all organisations that participated in our survey – your input will help us to better understand economic crime in Zambia. We hope our report is of use to you and your organisation in the fight against economic crime.

Introduction

We are pleased to present our eighth biennial Global Economic Crime Survey report and the second Zambia country report which aims to give you insight on corporate attitudes towards economic crime as well as seek to understand the trends and motives behind it. For the first time in Zambia, we are able to map a trend in economic crime having a set of 2014 results against which to measure the country's progress in the fight against economic crime.

Economic crime is the intentional use of deceit to deprive another of money, property or a legal right. It is a global phenomenon that cuts across all regions, industries and organisations. This year our survey received over 6,000 responses from 115 countries. The number of respondents from Zambia has increased from 83 responses in 2014 to 135 in 2016, accounting for 21% of respondents in Africa. These respondents consist of senior executives and representatives from both large and medium sized organisations. The majority of our respondents were from the Audit, Risk or Finance departments and/or working in the Financial Services, Communications or Manufacturing industries or in the Public Sector (Government or donor-funded institutions).

In 2014, the most predominant forms of economic crime were asset misappropriation, bribery and corruption and procurement fraud. However, this year's survey results have highlighted accounting fraud, cybercrime and money laundering as additional prevailing economic crimes. This shift is in line with the global survey results, although asset misappropriation is still the leading type of economic crime in Zambia with a high incidence level of 78%, followed by accounting fraud at 39%. Bribery and corruption and cybercrime have also prominently featured with incidence levels of 29% and 27%.

This year's survey drew a distinction between the traditional types of economic crime, such as asset misappropriation, accounting fraud and bribery and corruption and the imminent rise of tech savvy crimes such as cybercrime and money laundering – "crimes of the future". An interpretation of these results indicates a need for more vigilance in the business processes affected by these additional forms of crime.

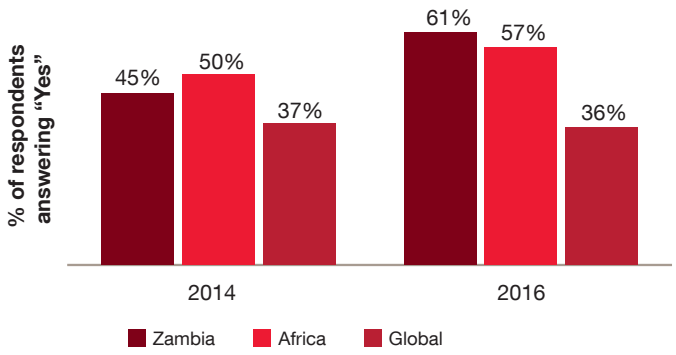
A more detailed description of the different types of crimes suffered in Zambia is explored in subsequent sections of this report. We also highlight areas where organisations can turn opportunity for crime into opportunity for growth.

The big picture

Economic crime on the rise in 2016

This year's survey results show that the global rate of reported economic crime has remained largely unchanged (36%), however the rate of economic crime reported in Zambia paints a very different picture. Economic crime has increased by a staggering 36% in Zambia, with almost two thirds of respondents (61%) reporting having experienced economic crime over the last 24 months. This is well above both the global and Africa averages of 36% and 57% respectively - as highlighted in the diagram below.

Figure 1 Organisations experiencing economic crime



Our survey respondents have told us that over the last 24 months, economic crime has thrived in Zambia, and the turbulent times the Zambian economy has faced over the last two years may have contributed to this position. Economic crime continues to be a key concern for organisations of all sizes, in every sector – not just in Zambia, but all over the world.

So which countries are experiencing economic crime the most and how is Zambia faring on the global scale? The 10 countries reporting the highest rates of crime are a mix of predominantly Western European and African countries. Zambia ranks third highest in the world (tied with Kenya), reporting a rate of 61% – below South Africa (69%) and France (68%).

While most regions reported lower rates of economic crime, Africa is one of the few regions where the incidences of economic crime has increased since our 2014 survey - reporting a 50% rate of incidence in 2014 and 57% in 2016.

In Africa, two countries reported increased rates of economic crime – Kenya (up 17% over 2014 results) and Zambia (up 36% over 2014 results).

Top 10 countries reporting economic crime

		2016	2014
1	South Africa	69%	69%
2	France	68%	55%
3	Zambia	61%	45%
4	Kenya	61%	52%
5	Spain	55%	51%
6	United Kingdom	55%	44%
7	Australia	52%	57%
8	Russian Federation	48%	60%
9	Belgium	45%	50%
10	Netherlands	45%	32%

It is also striking that cities in all three African countries featuring in the top 10 (South Africa, Zambia and Kenya) countries reporting economic crime also feature in *PwC's list of the top 20 cities of opportunity in Africa (as outlined in PwC's Into Africa: The continent's Cities of Opportunity* publication)[1] – in the markets we operate in, high opportunity for growth may also mean high opportunity for economic crime. In such environments, an organisation's approach to dealing with the risk of economic crime will determine which of these opportunities prevails.

[1] PwC's Into Africa: The continent's Cities of Opportunity publication is available for download at: http://www.pwc.com/gx/en/issues/high-growth-markets/africa-business-group/publications/into-africa.html

46%

of economic crime reported occurred in the Financial Services Sector

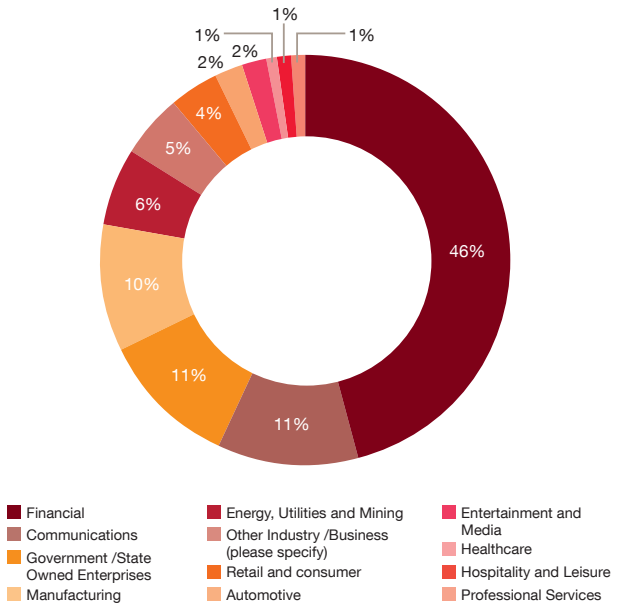
The opportunity thus exists for organisations, particularly in Africa, to take a view and apply stricter standards to their efforts at combatting economic crime – no matter the organisation's size or geographic diversity.

How can this be done? Is a one-size-fits-all approach tenable? We believe that organisations need to tailor their responses to their own circumstances – for Zambian organisations, gaining an in-depth understanding of the nature of economic crime in the Zambian market and in Zambian industries will help to do this.

Industry Spectrum

For our survey respondents who reported having suffered economic crime, the industries to which they belonged are set out in the figure below:

Figure 2 Respondents reporting economic crime in Zambia – by industry



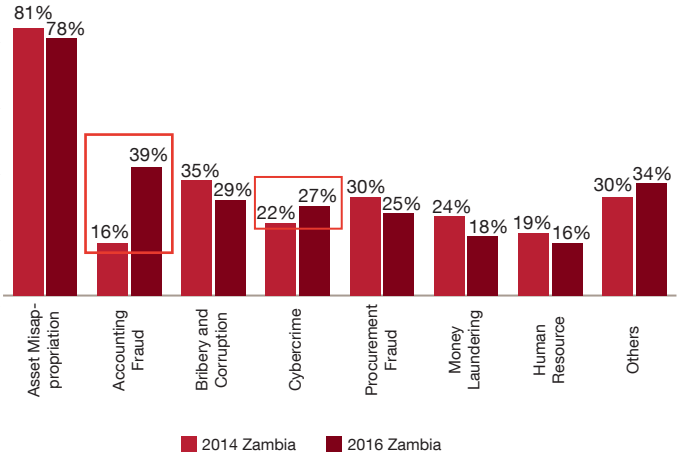
The financial services industry has traditionally been the most susceptible to economic crime. After all, it is arguably the one essential industry, as it serves the financial needs of all other industries. Globally too, the Financial Services industry experienced above average levels of economic crime (albeit a lower proportion – 27% of respondents who experienced economic crime globally were in the Financial Services Industry compared to 46% in Zambia). Other industries proportionally worse-affected by economic crime in Zambia include Communications, Government/State Owned Enterprises and Manufacturing. Whether globally or even just within Africa, these industries are within the top 5 industries worst affected by economic crime. Clearly, some industries are either by their nature or by virtue of their complexity of operations more easily targeted by fraudsters than others.

Globally, with the market evolving toward integrated business solutions, many traditionally non-financial services organisations are now coming into their own by providing for the financial requirements of their clientele in-house or expanding to mobile banking. Thus fraudsters seeking to "follow the cash" now have many more avenues to fulfil their objectives. Although Zambian organisations are still developing these financial services, they must ensure that they are fully aware and prepared for the associated risks. With the Zambian government seeking to diversify the Zambian economy and the potential growth in Manufacturing and Communications as a result, being alive to the vulnerabilities of organisations in these high-risk industries will help to harness their growth and make it sustainable.

Types of economic crime

The figure below highlights the most pervasive economic crimes in Zambia as reported by our respondents:

Figure 3 Types of economic crime suffered



Our survey results indicate that the nature of economic crime in Zambia has changed since 2014. While the top five most prevalent economic crimes in Zambia remain unchanged since 2014, the ranking of the individual crimes within the top five has changed.

Asset misappropriation, the perennial leader in this category, showed a slight decrease this year over 2014's statistics. This type of economic crime has traditionally been regarded as the easiest of frauds to detect – thus its prevalence from year to year is generally predictable. Yet organisations' efforts to mitigate its risk seem to fall flat, resulting in the rate of asset misappropriation far outweighing any other type of economic crime.

Accounting fraud has increased by 144% and cybercrime by 23% compared to reports of these crimes in 2014. Given the somewhat technical nature of these crimes we must ask ourselves: do we have appropriate controls in order to prevent these crimes or are we simply becoming less responsive to the risks our businesses face? Are we really detecting all the incidences our organisations might be experiencing? And the more important question: what should be done about this?

Bribery and corruption, procurement fraud, money laundering and human resources fraud have all maintained their positions among the top seven reported crimes in Zambia, but these too are reporting lower rates than previously.

It is also important to note the steady increase of other types of economic crime such as Tax Fraud for which the rate of crime is 10%, Insider Trading (8%) and IP Infringement (including theft of data) (4%).

2014:	**81%** Asset misappropriation	**35%** Bribery and Corruption	**30%** Procurement Fraud	**22%** Cybercrime	**16%** Accounting fraud
2016:	**78%** Asset misappropriation	**39%** Accounting fraud	**29%** Bribery and corruption	**27%** Cybercrime	**25%** Procurement fraud

While the rate of certain types of economic crime is much higher than others, not all types of fraud may pose the same level of threat to each industry. As we previously demonstrated, some industries are more vulnerable to economic crime than others, however all industries are at risk and where there are risks there are costs.

Frequency of incidences and Financial Damage

Zambia results in 2016 paint an interesting picture on how frequently organisations experience economic crime and how much it costs. On the one hand, more of our respondents said they experienced less than 10 incidents of economic crime in the last two years, compared to the previous survey. On the other, more of our respondents said they experienced more than 100 incidents of economic crime.

Similarly, with regard to the cost of each incident of economic crime, the number of respondents who have experienced both low value (less than US$100k) and high value incidences (over US$5m) has increased in the last two years, compared to our previous survey.

This is closely tied to another key theme in this survey: the opportunity to commit fraud. The results of our survey suggest that fraudsters will take whichever opportunity they can to commit fraud, whether the returns are of high or low value. Those who feel they are able to escape detection seem to then escalate their efforts, either committing repeat low value frauds (thereby increasing the number of incidents suffered) or committing higher value frauds (therefore increasing the losses due to economic crime).

Figure 4 Number of incidents of economic crime

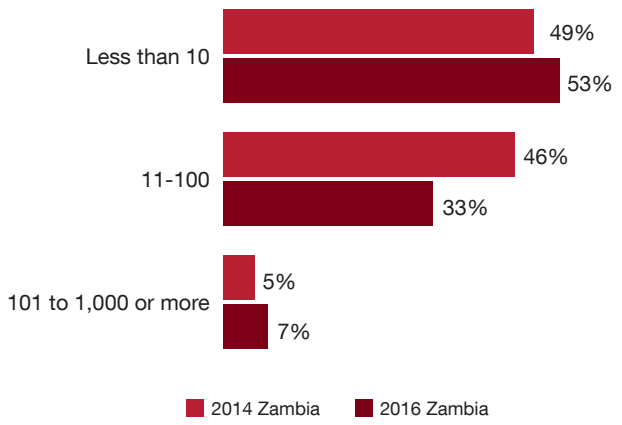
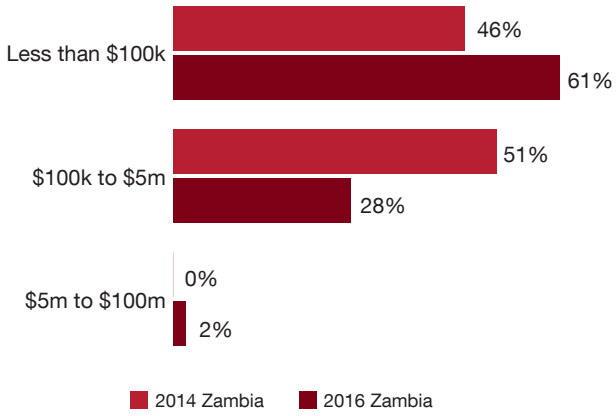


Figure 5 Estimated amount lost due to economic crime



The costs above are likely to capture only the financial losses due to economic crime. The true costs of economic crime are difficult to estimate. Business disruptions, reputational damage, remedial measures, investigative and preventative interventions, regulatory fines and legal fees, lost investment or growth opportunities and the time spent by management in dealing with the aftermath among others all have an impact. These costs can be enormous and are difficult, if not impossible, to quantify.

Turning opportunity for crime into opportunity for growth

This year our survey explores managing the risks associated with technology and integrating old-school ethical conduct into decision making.

We will not only discuss the opportunities that enable economic crimes to be perpetrated, but more importantly the opportunities available to organisations to proactively counter these attacks.

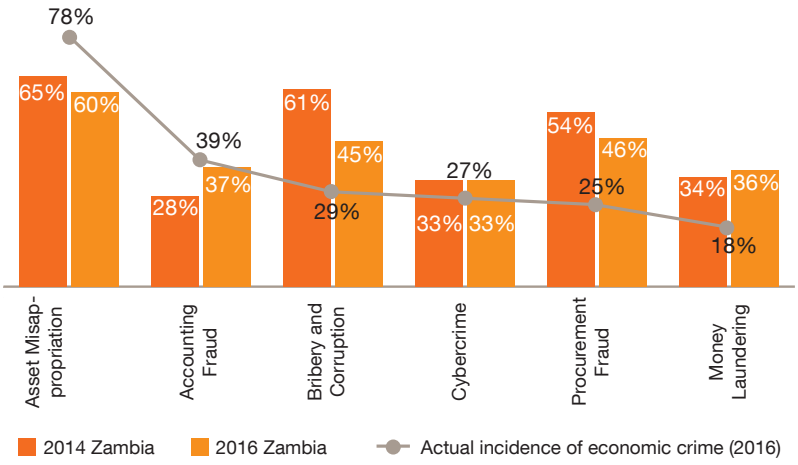
By focusing on the things you can't control (like the continuity of economic crime), we hope to emphasize the things you can control, such as implanting sophisticated measures that can not only reduce risks, but also deliver business benefits.

Traditional types of economic crime

Our respondents expect to suffer more incidences of Accounting Fraud and Money Laundering in the next 24 months.

The graph below highlights the top six types of economic crime reported in Zambia and our respondents' perception with regard to the likelihood that they will experience these crimes in future. These perceptions are also compared to the actual rate of economic crime reported between 2014 and 2016.

Figure 6 Perceived likelihood of the following economic crimes in the next 24 months vs actual incidence in 2016?



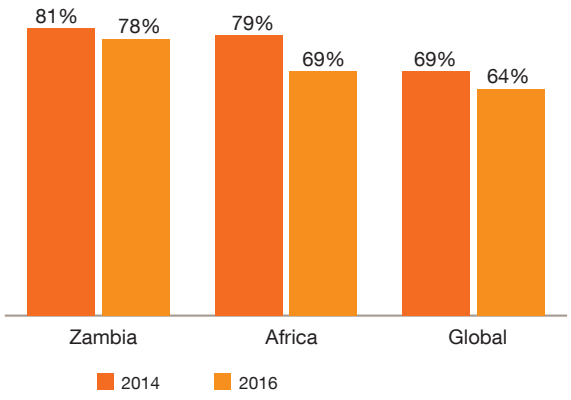
While respondents have told us that they believe they are less likely to suffer most types of economic crime in the next 24 months, they expect the incidence of accounting fraud and money laundering to increase in the coming period. In addition, it is interesting to note that for both asset misappropriation and accounting fraud, respondents in 2014 believed they would face a lower incidence than the actual in 2016. The opposite was true of Bribery and Corruption, Cybercrime, Procurement Fraud and Money Laundering – respondents in 2014 believed they would suffer more incidences than they actually did. On the one hand, this could be seen as a positive outcome – with incidence levels also having dropped for Bribery and Corruption and Procurement Fraud.

However, this could also raise concerns over the effectiveness of detection mechanisms in our organisations – the sophistication of fraudsters is growing constantly, detection mechanisms need to be just as agile (if not more) and evolve constantly to function effectively. Unless organisations have complete faith that their detection mechanisms are robust, organisations should be careful not to take a false sense of security from these results.

Asset Misappropriation

Asset Misappropriation is by far the most common economic crime, experienced by 78% of organisations reporting any economic crime over the last two years and double the next-most frequently reported crime, accounting fraud (39%). The survey results show a downward trend in the reported rate of asset misappropriation across the globe; Zambia's reported rate has decreased from 81% (in 2014) to 78% (in 2016). However this is still high when compared to the Africa and Global averages of 69% and 64% respectively.

Figure 7 Asset Misappropriation



While the overall reduction of asset misappropriation across the region may equate to a tightening of organisational controls, it could instead mean that complacency is setting in. Perhaps what was once the easiest crime to detect is slowly becoming less so.

As an economic crime, Asset Misappropriation attacks fundamental business processes including distribution, logistics and warehousing. Another function commonly threatened by asset misappropriation is the expense reporting process. The crime impacts cash disbursements and potentially leads to collateral damage to bookkeeping and records. Thus, while the individual cost of each fraud incident may be lower than it is for other types of economic crimes, the frequency and knock-on effects of the threat requires organisations to be vigilant.

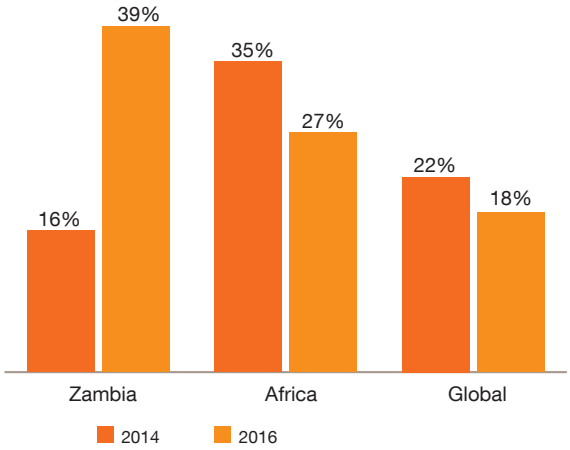
Asset misappropriation is the most common economic crime and is usually the easiest to commit because it is committed by individuals who have been entrusted with the property of an organisation. Since they already have access to the organisation's property, they have the best opportunity to commit asset misappropriation.

Even if crimes committed are low in value or simple in nature (e.g., stealing stationery or inventory), these opportunistic economic crimes can transform the culture of the organisation and become systemic. Opportunity can also lead to repeat occurrences and escalate to more significant, costly frauds.

Accounting Fraud

Accounting fraud, which includes misleading or falsely prepared financial statements, has always been one of the major crimes reported in our survey. It can deceive banks, lenders, vendors and investors to make risky or misguided decisions. Due to the ubiquitous use of financial statements and financial data in business operations, this kind of economic crime impacts a variety of business processes. While the rest of the globe reports having experienced lower rates of accounting fraud, this type of economic crime has significantly increased in Zambia from 16% to 39% (an increase of 144% since our last survey). What has caused this increase and which industries are at risk?

Figure 8 Accounting Fraud

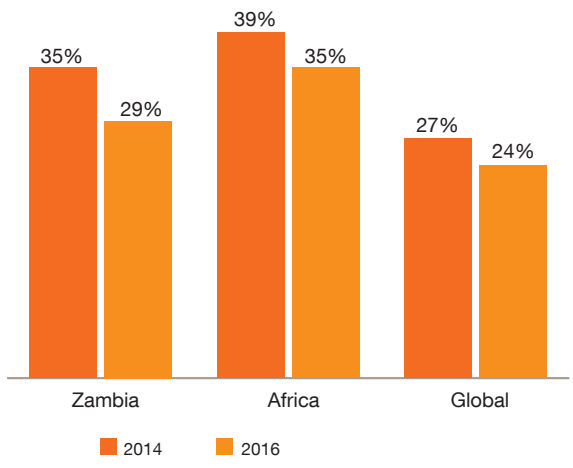


Although the most affected industry is Financial Services (59%), the rate of accounting fraud reported in this sector has actually decreased by 11% since 2014. This is also the case for the Communications industry which has seen a 44% decrease since 2014. Thus, the key driver for the sharp increase in the rate of accounting fraud overall is due to an increase in this type of crime reported across all the other sectors (many of which in 2014 reported having experienced zero incidents) and in particular, Manufacturing and Government/State Owned Enterprises.

The truth is that accounting fraud can be used to hide all types of economic crime – this might be a possible explanation for the increased rate of accounting fraud. It is frequently used to conceal the theft of inventory or cash (asset misappropriation) or even to perpetrate it (for instance, the misreporting of sales or costs to commit tax fraud). As bribes and related payments are not usually recorded accurately in financial statements, a bribery and corruption issue can quickly turn into an accounting fraud issue as well.

However, while accounting fraud may be used to hide other types of economic crime, accounting fraud may also be committed for its own sake – for instance, misreporting of financial or operational information to artificially meet reward-linked targets or for the sake of career growth. When this does happen, it can be very destabilising to the business, especially where senior management are involved. For an organisation, apart from the distress in resolving the potential tax and regulatory implications and dealing with the management issues that may arise, misreporting of financial results can lead investors to question, delay or even reverse their investment decisions – this has long term implications for growth and development. However, due to the wide range of users of financial statements and depending on the depth and scale of the accounting fraud, the implications could be much wider.

Figure 9 Bribery and Corruption



Bribery and Corruption

There has been a downward trend in the rate of bribery and corruption in 2016 when compared to 2014. The rate of bribery reported in Zambia (29%) is below the Africa average (35%) but above the global average (24%).

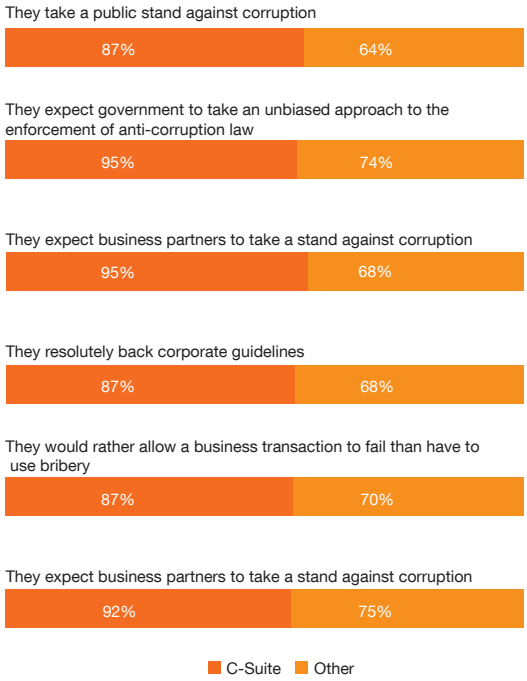
The number of reporting organisations asked to pay a bribe in Zambia has also decreased by 68% over the last 24 months, as well as the number of opportunities lost to competitors believed to have paid a bribe, down by 31% since 2014. While the number of respondents experiencing bribery and corruption has decreased, some are still reporting to have been asked to pay a bribe (7%) or believe they have lost an opportunity to a competitor believed to pay a bribe (15%).

Consider that the only industry to have experienced a decrease in bribery and corruption is Financial Services. The reported rates for all other industries are either unchanged or have increased. One could argue that bribery and corruption is actually on the rise in Zambia and now poses a greater risk across the industry spectrum. Nonetheless, bribery and corruption is ranked third in Zambia. In addition, these crimes are notoriously difficult to detect and combined with the increase in accounting fraud, our perception is that the risk of bribery and corruption is still very high.

Perceptions on bribery and corruption

Our survey also measured our respondent's perception of our respondents to how top level management deals with corruption in Zambia. We compared C-Suite's perception of bribery and corruption with that of other staff members and the results show some interesting discrepancies. Our findings are highlighted in the diagram alongside.

Figure 10 How do your colleagues perceive the way top level management deals with corruption? (Zambia)



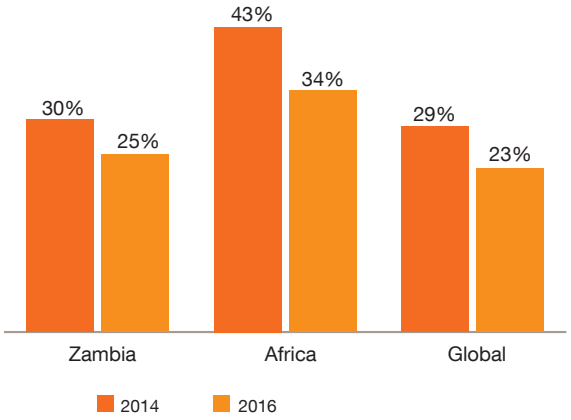
One of the largest discrepancies between C-Suite and other staff members concerns top level management's public stand against corruption. While 87% of C-Suite respondents believe that top level management takes a public stand, only 64% of other staff think the same. The results also show that only 70% of staff believe top level management would rather allow a business transaction to fail than resort to bribery. Only 68% of staff respondents believe that top level management resolutely backs corporate guidelines.

This discrepancy between the perception of C-suite and Other staff may lead us to question whether the corporate values that C-suite obviously hold are sufficiently reflected in their "tone" within the business or whether they are adequately communicated to staff. It can also point to a gap between the understanding the C-suite have of their business and the experience of the rest of the organisation. Until these gaps and discrepancies are resolved and both C-suite and the rest of the organisation are united in their outlook and perceptions, bribery and corruption will continue to be a high risk area for organisations in Zambia.

Procurement Fraud

Procurement fraud is a double threat. Not only does it victimise businesses acquiring goods and services, it also prevents companies from competing fairly and successfully for business opportunities subject to a commercial or public tender process. Procurement fraud was first counted as a separate category in 2014 and across the globe, respondents have reported lower rates compared to 2014. Zambia's rate (25%) has decreased by 17% since 2014, and is well below the average for Africa (34%) to become more aligned with the global average (23%).

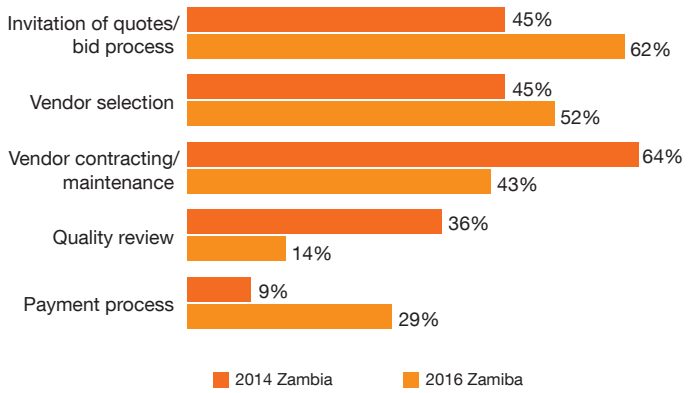
Figure 11 Procurement Fraud



Generally speaking, when an organisation goes into a commercial or public tender process or seeks to acquire goods and services (which are common business processes across all industries), the potential for procurement fraud exists. Our results show that Government/State Owned Enterprises have been most affected by procurement fraud (38%). The Manufacturing and Energy, Utilities and Mining sectors both experienced a 57% increase in procurement fraud, while Financial Services saw a decrease from 55% in 2014 to 24% in 2016. Procurement is a lengthy process for which there are many stages, it is therefore important to understand the areas in which the fraud is occurring.

Areas of impact

Figure 12 In which areas did the procurement fraud primarily occur?



Our results show that in the last two years, the stage at which procurement fraud primarily occurs has moved from the contracting stage to the pre-contracting stage. The pre-contracting stage begins with the invitation of quotes/bid process (up by 38% from 2014) and the vendor selection stage (up by 16% from 2014). It is also important to note the large increase in procurement fraud occurring at the payment process stage, up by an alarming rate of 222% from 2014. Both these trends are extremely worrying as they point to poor procurement practices not just at the end of the procurement cycle but also at its start. For an institution suffering fraud at both of these stages of the procurement process, this trend could point to deficiencies in corporate culture and corporate controls, both of which are vital tools in the detection of economic crime.

Knowing the risky areas in the procurement process is important. This knowledge can help identify threats which organisations should ensure they address. These threats can be either external or internal. What can your organisation do about them? Our focus will be on the threats that are most within your control: the internal threat.

Internal threats to the procurement process

The threat from within is often overlooked. This is especially significant in cultures where loyalty to family, schoolmates, local community or even national pride are strong influences and stronger perhaps than corporate policy statements or codes of conduct. For example, an individual within the purchasing and supply department may have a pre-existing relationship with a vendor who wants to win business from the organisation. The insider provides information on the bidding process, such as the bid amounts of competitors, to ensure an advantage for their preferred bidder. Or, the insider could approve a price higher than necessary.

Alternately, your controls may not function as planned. It is common for employees in approval roles to acquiesce to pressure from "the boss" to process payments that do not meet all aspects of policy and procedure. This tension between an executive's loyalty to company standards versus their ability to influence staff decisions is a real and continuing threat to controls.

Crimes of the future

86%

of Cybercrime incidents in Zambia have occurred in the Financial Services Sector

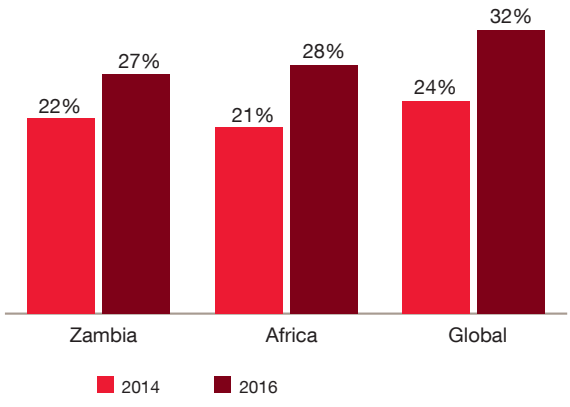
Cybercrime: risks and opportunities

Cybercrime has been on a steady increase since its debut in our survey back in 2011. The rise of technology has exposed organisations to a number of threats, the key ones being:

- **Insiders** — not only employees but also trusted third parties with access to sensitive data
- **Organised crime syndicates** — threats include theft of financial or personally identifiable information (sometimes with the collusion of insiders); victims often include financial institutions, retailers, medical and hospitality companies
- **Hacktivists** — threats include service disruptions or reputational damage; victims often include high-profile organisations and governments

The nature of cybercrime is such that the threat actors can target any country in the world, regardless of their own location. This means that whether or not the cybercrime threat exists within Zambia, Zambia is at risk. Our survey results show that cybercrime has increased by 23% in Zambia (from 22% in 2014 to 27% in 2016), a trend which we are seeing globally – as shown in the diagram below:

Figure 13 Cybercrime



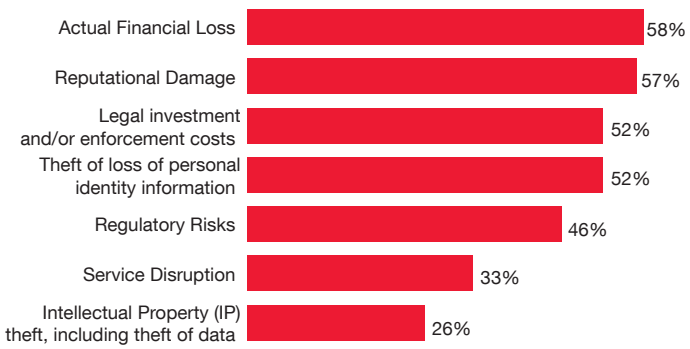
Financial Services is a clear leader in this category (this is also true globally and within Africa) accounting for 86% of the total cybercrime incidents reported by Zambian respondents in 2016. The Communications industry has experienced a significant decrease in cybercrime over the last 24 months, while Government/State Owned Enterprises have experienced an increase in this type of crime whereas the sector previously reported zero incidents in 2014. The Communications industry and Government/State-Owned Enterprises in Africa also seem more vulnerable to this type of economic crime compared to other industries.

There are many associated risks with cybercrime and the increased rate of its occurrence has had both a financial and non-financial impact on organisations.

Impact of cybercrime

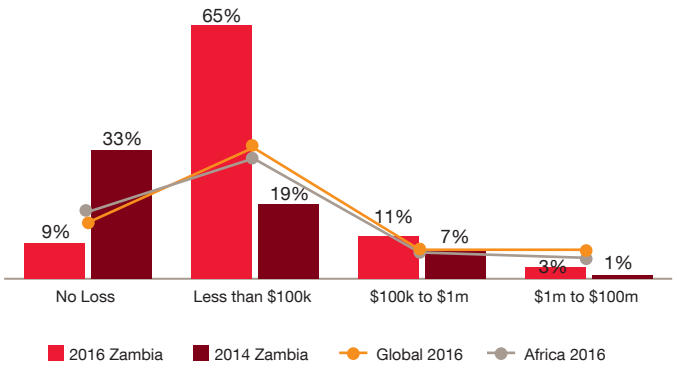
Almost half of our respondents (49%) stated that their perception of the risks of cybercrime to their organisation have increased since 2014 - and with good reason. Not only is the rate of cybercrime increasing worldwide but so is its impact. The areas experiencing a medium-to-high impact as a result of cybercrime are highlighted in the diagram below, with the most impact being felt in terms of financial loss (58%) and reputational damage (57%).

Figure 14 If cybercrime has affected your organisation in the last 24 months, which of the following aspects had a medium-to-high impact? (Zambia)



With regard to cybercrime, our respondents reported the highest impact to be financial loss. We asked respondents to quantify this loss – the results show that the quantum of financial losses have increased greatly from 2014 and the number of organisations reporting no loss from cybercrime has dropped sharply (from 33% in 2014 to 9% in 2016). Almost two thirds (65%) suffered a loss of below $100,000 compared to a much lower 19% in 2014 and the number of respondents suffering losses of between $100k-$1m has also climbed from 7% in 2014 to 11% in 2016. A growing number of cybercrime incidents have resulted in losses over $1 million (3% in 2016 from 1% in 2014). These results are a cause for concern and show that the threat of cybercrime is increasing in Zambia.

Figure 15 Financial loss due to cybercrime (USD)



While Zambian organisations report to have suffered smaller value financial losses than their counterparts globally (who experience more high value incidents over $1m), the stakes are still extremely high. Considering the current state of the Zambian economy, any financial loss could pose a serious concern to both small and large organisations.

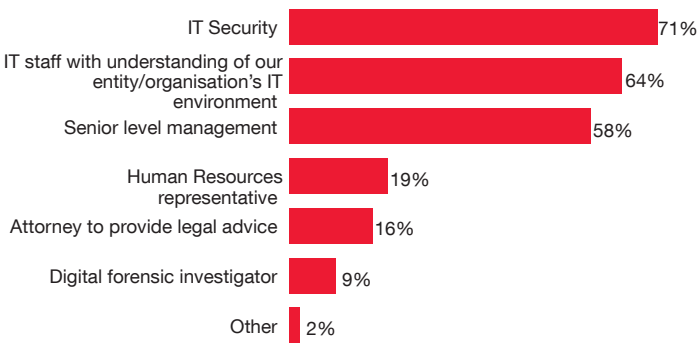
Financial loss is not the only threat. More than half of our respondents (57%) said that their reputation also suffered heavy damage due to cybercrime. It is common for top level management to focus on the numbers only, forgetting the significance of the intangible risks as well. With the consequences being so high, how prepared are organisations to handle incidents of cybercrime?

Organisations' readiness to deal with cybercrime

Our survey revealed that just under half (49%) of board members in Zambia request information about their organisation's state of cyber-readiness, while 18% do not request this information or do not feel the need to do so. Only 44% of respondents have a fully operational incident response plan, most of them in the heavily regulated financial services industry, while 10% have no plan at all, nor do they intend to implement one.

Should a cyber-crisis arise, only 51% of companies have personnel that are "fully trained" to act as first responders and the overwhelming majority are IT staff (71%). Additionally, only 9% of incident response teams included a digital forensic investigator.

Figure 16 First Responder Team (Zambia)



The results suggest that cyber-crime defence is still viewed as an "IT issue" as opposed to an organisation-wide issue. It is important for organisations to realise that the human or user aspect of an IT system is just at risk of breach (or even more) as the IT system controls themselves. This means that any user of an IT system, whether they be IT personnel or a till manager at a point-of-sale terminal, could expose your organisation to a cyber-crime threat. Indeed, social engineering (psychologically manipulating an individual into breaking security procedures or providing confidential information) is a technique often used by perpetrators of cybercrimes. As such, it is not sufficient to view cybercrime as an IT issue. The entire organisation must be on guard and prepared to deal with cybercrime threats.

These results also suggest that many organisations, in their understandable haste to contain the breach and get their systems up and working again, are at risk of overlooking potentially crucial evidence which could later hamper their ability to prosecute and, more importantly, to understand how the breach occurred.

When it comes to seeking help from local law enforcement, the results show great pessimism. Only 14% of respondents said they had confidence in local law enforcement's ability to effectively investigate cybercrime, while over two thirds (67%) did not. The table below shows the 10 countries reporting the lowest rate of confidence in law enforcements ability to investigate cybercrime. Zambia ranks third highest among our global survey respondents.

Top 10 countries reporting that they do not believe local law enforcement agencies have the required skill and resources to investigate cybercrime

1	Kenya	73%
2	South Africa	70%
3	Zambia	67%
4	Nigeria	62%
5	Luxembourg	59%
6	United States	58%
7	Ukraine	57%
8	United Kingdom	57%
9	Mexico	57%
10	Turkey	56%

There are a few possible explanations for these low confidence numbers. Cybercrime's rapid evolution requires a degree of sophistication that is often beyond the resources available to law enforcement agencies. Worth noting in particular is the fact that the top 10 countries exhibiting low confidence levels include developed economies such as the United States, the United Kingdom and Luxembourg, thus dispelling the notion that this might be an issue only prevalent in developing or underdeveloped countries.

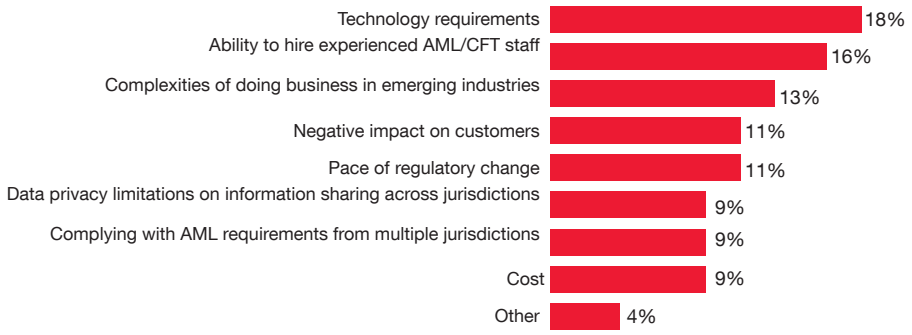
The truth is, protection from cybercrime must start at home. While IT has a critical role to play in detecting and attempting to deflect an attack, it is important to note that IT threats and mitigations are the responsibility of the entire organisation. For example executives should implement security awareness programs and budget for spending on security, while legal teams should be fully aware of factors that can void cyber insurance.

A cyber crisis is one of the most complex and challenging issues an organisation can face. Cyber breaches require sophisticated communications and investigative strategies — including forensic and analytical capabilities. However, a company's degree of readiness to handle a cyber-crisis can also be a marker of competitive advantage and ultimately, its survival.

Anti-Money Laundering: the fast changing regulatory environment

Our survey results show that over three quarters (78%) of respondents have performed an Anti-Money Laundering/ Counter Terrorist Financing ("AML/ CTF") risk assessment over the last 24 months. Just under half of the respondents who identified any suspicious activity did so by using internal reports from sales staff and/or relationship managers. Even so, there are still a number of challenges. The most significant challenges in relation to complying with local AML/CTF requirements are highlighted in the figure alongside:

Figure 17 What are the most significant challenges in relation to complying with local AML/CTF requirements? (Zambia)



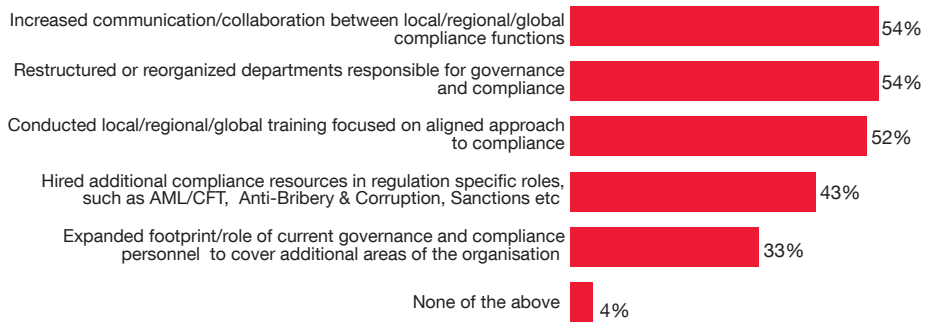
The most significant challenge reported by our respondents is the technological requirements (18%), followed by the lack of experienced AML/CTF staff (16%). Respondents also reported issues relating to their AML/CTF systems, in particular data quality and maintenance of client information in electronic format and the complexity of implementing/ upgrading systems. Such challenges need to be addressed as soon as possible as money laundering facilitates economic crime by holding/transferring funds in order to commit crimes such as corruption or tax evasion. It can also have a major effect on an organisation's reputation.

Any organisation that facilitates a financial transaction is at risk and many are not up to speed on the requirements they must meet. As regulation becomes more complex, the cost of compliance continues to rise and keeping up with regulatory developments can be a difficult task. However, installing a robust and up-to-date AML programme can yield benefits in relation to both AML and other compliance functions such as anti-bribery and fraud monitoring and response. So how can organisations implement an effective AML programme?

People and Process

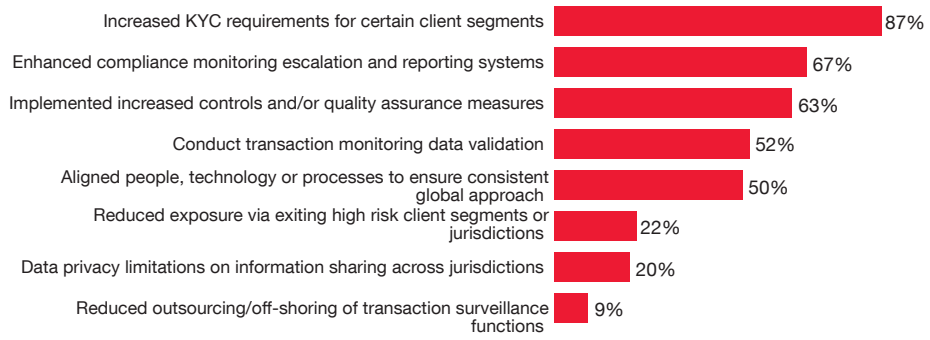
In AML compliance, your first line of defence is not only having the right technology but also the right people with the right skills, both of which pose a significant challenge for our respondents. So how are organisations addressing this issue?

Figure 18 Measures implemented to address increased regulatory expectations (Zambia)



Some organisations are addressing the skills challenge through training of in-house resources (52%), while others are increasing communication/collaboration across geographical compliance functions (54%) or restructuring departments responsible for compliance (54%). Risk assessments are critical as they identify and measure risk areas, develop processes to help mitigate the risks and apply control measures and they are conducted by over three quarters of respondents (78%). Other methods being used to reduce AML/CTF risks are highlighted in the diagram alongside:

Figure 19 Activities implemented to reduce AML/CTF risks (Zambia)



Majority of respondents are increasing KYC requirements (87%), while others are either enhancing compliance and reporting systems (67%) or increasing controls (63%). The key to safeguarding your organisations from AML attacks is to keep monitoring for suspicious activity and to ensure that risk assessments are conducted on a periodic basis. Special attention should be paid to business relationships/transactions conducted with persons residing in locations with weak AML regulations.

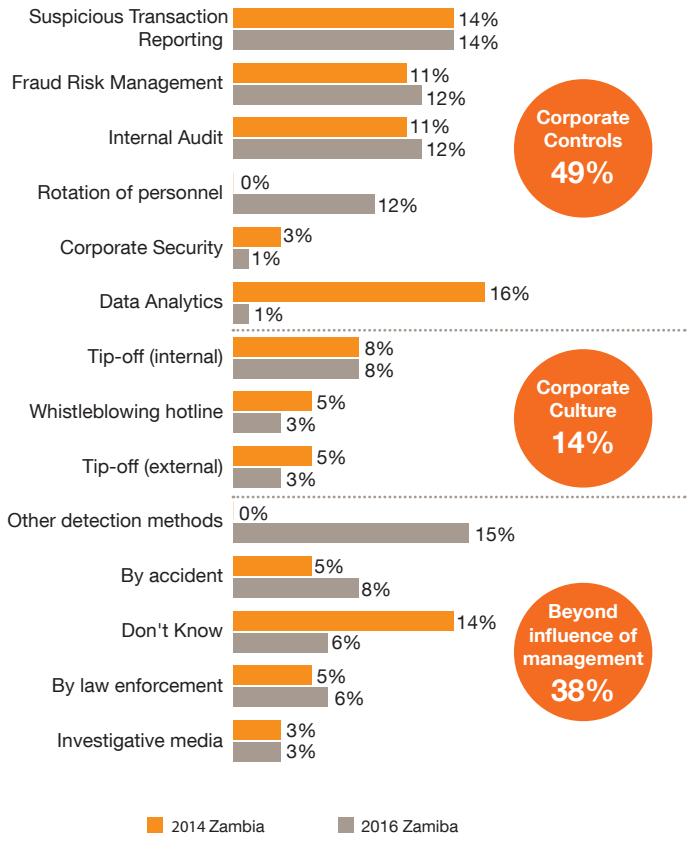
Detecting economic crime and identifying the perpetrator

The low percentage of respondents detecting economic crimes through corporate culture indicates a gap between corporate values and corporate behaviour.

Detection

The most common method of detection for organisations experiencing economic crime is through corporate controls (49%). However, over a third of organisations (38%) appear to take a back seat approach and rely on factors beyond their influence/control in order to detect fraud, with only 14% of respondents detecting economic crime through corporate culture. This indicates a gap between corporate values and behaviour.

Figure 20 Detecting economic crime



The majority of respondents use techniques such as suspicious transaction reporting (14%), fraud risk management (12%) and internal audits (12%) to identify fraudulent behaviour. Fewer organisations rely on data analytics compared to 2014, used by only 1% of respondents in 2016 compared to 16% in 2014 (the most used method then). Given that data analytics is a rather simple and quick process which, if used correctly, can easily uncover discrepancies and/or highlight potential fraudulent activity, the fact that it is not being used as a method to detect crime raises questions. How well are organisations using the different types of data they generate on a daily basis and are they making the best use of it?

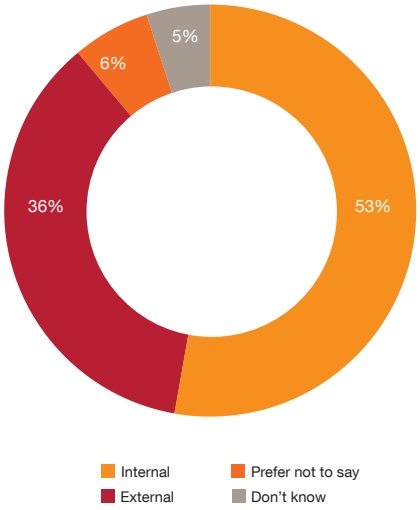
Further, when asked how often fraud risk assessments are carried out, only 23% of respondents conduct quarterly assessments, while 21% perform fraud risk assessments on an annual basis. This is worrying as it indicates that some organisations are perhaps not taking economic crime as seriously as they should. Detecting fraud is the first step, but what methods are organisations turning to in order to identify who is responsible and how to tackle it?

The Perpetrator

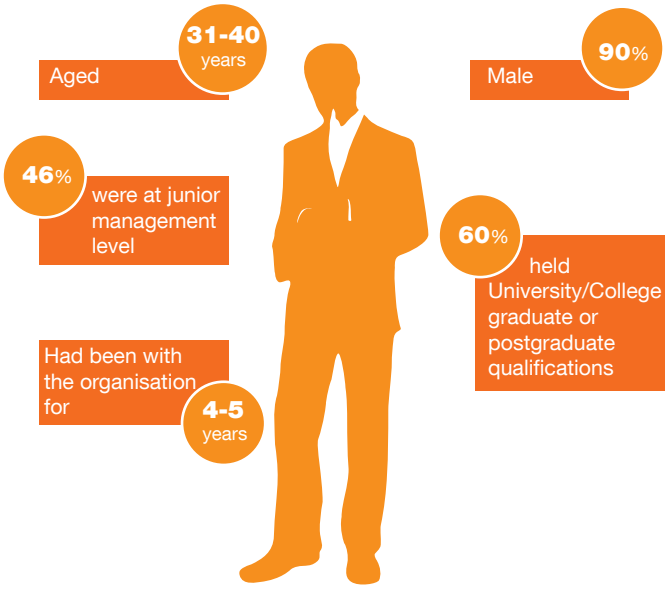
In this section we will explore the characteristics of a fraudster and their motivations as well as organisations' responses to them.

The main perpetrator of economic crime continues to be the internal fraudster, albeit at a lower reported rate than previously (53% in comparison to 65% in 2014), while 36% of economic crime is committed by external fraudsters.

Figure 21 Main perpetrator of economic crime (Zambia)



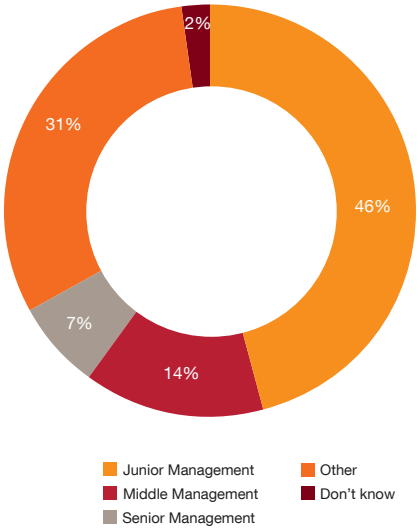
Profile of a fraudster



Internal Fraudster

With the majority of economic crimes being committed by internal fraudsters, it is crucial for organisations to be aware of where the highest risk lies. Almost half of internal perpetrators (46%) originate from junior management.

Figure 22 Level of internal fraudster (Zambia)



According to our survey respondents, most internal fraudsters possess the following characteristics:

- Aged 31-40 years
- Male (90%)
- Had been in the organisation for 3-5 years
- 60% held University/College graduate or postgraduate qualifications

These characteristics are not unique to Zambia – both globally and in Africa, the typical fraudster exhibits the similar characteristics. What is unique to Africa is the higher proportion of incidences of economic crime from internal perpetrators versus external perpetrators. This may point to differences in corporate culture and the opportunity to commit fraud.

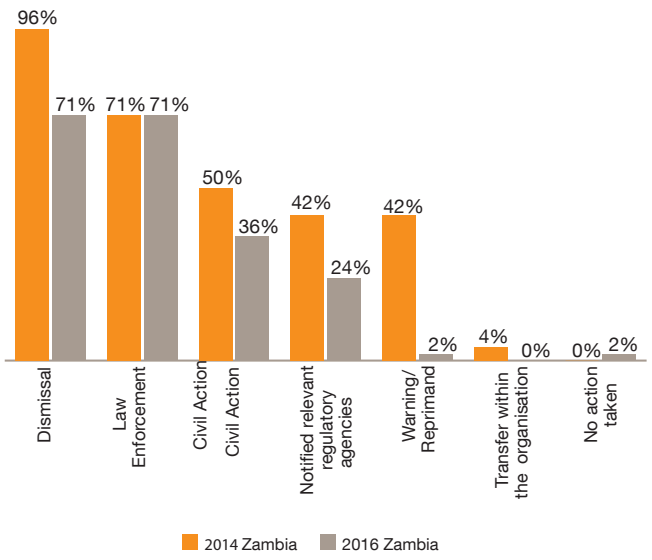
Which factors may contribute to the commission of fraud by an internal party? Practitioners commonly refer to a 'Fraud Triangle'. The three elements that are often present when a perpetrator commits a fraud are: pressure, opportunity and rationalisation.

Almost two thirds of respondents (60%) reported that opportunity or the ability to commit the crime was the factor that most contributed to economic crime by an internal fraudster. Perhaps this is due to the perpetrator having been entrusted with responsibility/stewardship over the organisation's assets or perhaps a lack of proper internal controls. While 26% believe economic crime is committed because the perpetrator can rationalize the justification for the crime, 10% believe fraud is committed due to pressures on them to perform (e.g., a bonus scheme linked to monthly targets).

Of the three factors, opportunity is the one most within an organisation's control. While life's pressures and the ability to rationalise may swirl around employees, if an organisation can limit the opportunity, it may be able to stop the fraud before it starts. However, where economic crime has occurred, the organisation's response is crucial as this will set a precedent and deter other potential fraudsters.

The majority of respondents deal with incidents of economic crime by dismissing the main perpetrator and informing law enforcement (71%), with just over a third taking civil action (36%).

Figure 23 Action against main internal perpetrator



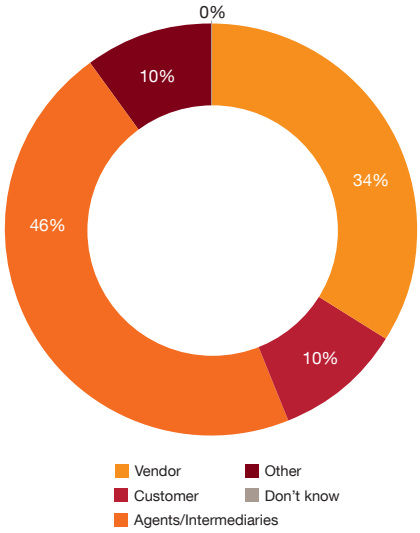
The downward trend for each of the actions in the diagram above is extremely worrying with almost all showing a decrease since 2014 and some organisations choosing to take no action (2%). The fact that organisations are taking less action against internal perpetrators will most likely increase the chance of economic crime occurring because there are fewer consequences.

Organisations can take this opportunity to rethink their control structures and return to fundamentals. Creating a culture of controls and risk awareness rather than ritualised activity, supplemented by zero tolerance for dishonest practices, can help insulate organisations from avoidable losses due to internal fraud.

External Fraudster

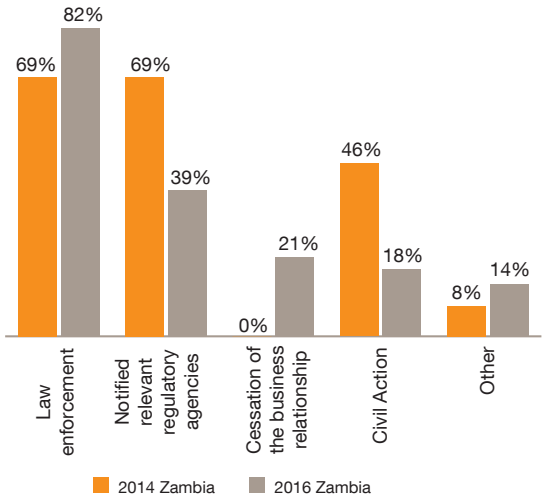
This year's results show that 36% of economic crime is committed by external actors. The main perpetrators of external fraud are highlighted in the diagram below:

Figure 24 Main pepetrator of external fraud (Zambia)



Just under half of respondents (46%) said to have suffered from economic crime as a result of external factors other than customers, agents/intermediaries or vendors. Some of the other external perpetrators listed by our respondents include ATM/POS skimmers, external criminals/fraudsters not linked to the organisation, taxpayers and unknown individuals. So, where the external perpetrator is known, how are organisations dealing with them?

Figure 25 Action against external perpetrators



With regards to external perpetrators, most respondents (82%) choose to involve law enforcement. Compared to 2014, a growing number of respondents are choosing to cease the business relationships with these external parties – this is commendable as it displays a no-tolerance policy and is likely to have longer term knock-on effects. However, unless respondents choose to take further action with respect to these external fraudsters (e.g. notifying law enforcement or regulators), they may be leaving others exposed to the risk of fraud from the same party.

Of comfort, however, is the result in our survey that the decision to inform law enforcement ranks high for action taken against both external and internal fraudsters, 82% and 71% respectively. This is despite the fact that more than half (55%) of respondents do not believe that local law enforcement agencies are adequately resourced or trained to investigate and prosecute economic crime.

There appears to be an unwillingness to inform regulatory agencies with only 39% of respondents choosing to do so.

With there being little faith in the ability of local law enforcement and/or regulatory agencies to tackle economic crime, what methods are organisations turning to as an alternative (we explore this question in more detail later in this report)?

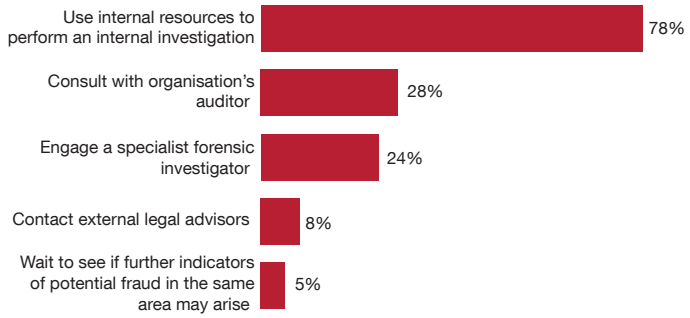
Handling incidents of economic crime: The way forward

Independent investigations conducted by specialists can strengthen both business processes and internal capacity to detect and handle incidents of economic crime

Action

Most organisations (78%) prefer to use internal resources to perform an internal investigation once economic crime has been detected; the second most popular option is to consult with the organisation's auditor (28%). However, it is important to note that both the decision to carry out an internal investigation and/or consult the organisation's auditor can have its limitations if not combined with engaging a specialist forensic investigator.

Figure 26 Action taken once fraud is identified (Zambia)



Internal investigations

Conducting an internal investigation is by far the most common method for investigating economic crime with over three quarters of respondents (78%) choosing this method. From our experience, these internal investigations are often undertaken by internal audit teams or in-house investigation teams. While well-run internal audit or internal investigation functions can be the first line of defence when tackling economic crime, they too have their own limitations. First, it is not always easy to ensure the independence of an internal investigation team. This is particularly true with smaller markets where it is almost impossible to avoid day-to-day contact with subjects of an internal audit or investigation or members of management who are tasked with functions that are the subject of an internal review. Internal investigators are human after all and the possibility of being ostracized in a work environment may pose a threat to the independence of even the best internal investigator.

Another threat to a robust internal investigation is familiarity, either with colleagues or the controls being reviewed. We have frequently observed unusual or inappropriate business practices becoming "institutionalized" over time and then manipulated to the advantage of a fraudster. Sometimes all it takes is an independent eye or a fresh perspective to point this out. In addition, internal audit teams may deteriorate in their value if considered to be a "routine" function. A successful internal investigation team should therefore constantly evolve and employ innovative and creative techniques. This will introduce an element of unpredictability into their work and increase the likelihood of preventing and detecting economic crime.

External auditors

Just over one quarter (28%) of respondents chose to consult external auditors once fraud had been detected. While recommendations or reports from statutory audits may point towards potential issues in an organisation, they may just as easily fail to do so. This is because their objectives and approach are not necessarily geared to detection of fraud.

The scope and objective of a statutory audit is to provide an opinion on whether the financial statements present a "true and fair" reflection of the company's financial performance and financial position over the period covered and not necessarily to detect and/or investigate fraud. Audit work is carried out on a sample basis, thus auditors will rarely (if ever) cover 100% of the transactions a business enters. As a result, the opinion they provide is on whether the financial statements are free from material misstatement, whether caused by fraud or error. In the context of a statutory audit, the tendency may be to disregard immaterial errors or frauds. However, "immaterial" misstatements often mask deeper underlying issues and may be a precursor to a larger event of economic crime.

Furthermore, economic crime by its nature is difficult to detect because deliberate attempts are made to conceal it. It could involve forgery of documents or calculated attempts by the perpetrators to mislead the audit team. As such, the mandate of an audit may not be sufficient to investigate economic crime, especially if there is collusion by management to conceal evidence. It is therefore crucial to understand the mandate and limitations of a statutory audit when considering how to investigate economic crime.

Specialist forensic investigator

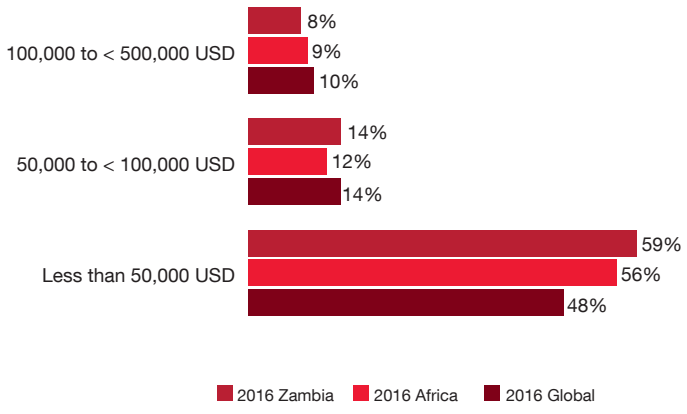
Only 24% of respondents chose to engage a specialist forensic investigator after detecting fraud. Reviews conducted by external parties to identify fraud risks or investigate economic crime can be of good value to an organisation. For one, they are independent and will not be a victim to any bias or hierarchical concerns which an internal investigation/review would be subject to because their work will be impartial and factual. By bringing together best practices from a variety of industries and backgrounds, independent investigations conducted by specialists can strengthen both business processes and the internal capacity to detect and handle incidents of economic crime. Their work can include helping to implement the necessary measures to manage fraud risks and thus prevent fraud. Specialist skills such as conducting interviews in an investigation or collecting/handling evidence may also enhance the organisation's ability to manage the uncovered matters. Digital forensics and its use in gathering evidence is a prime example of this type of specialist skill.

In addition, seeking the involvement of an independent team means they will have the focus and time required to thoroughly query the matters at hand. There is also a lower likelihood of them being misled with an explanation that staff are accustomed to giving an internal investigation team. Their recommendations will be on the basis of best practice and industry benchmarks rather than internal policies or inappropriate but established norms. In fact, an external perspective could bring about changes to these norms and yield long term benefits. Each of these techniques come at a cost, and cost considerations play a key role when organisations seek to determine a way forward once an incident of economic crime has been detected. Our survey also shows how much organisations spend on investigating economic crime and the results are included in the sections below.

The costs

Globally, almost half the organisations surveyed indicated that they spend less than $50,000 to investigate economic crime but this varies depending on the severity of the fraud and the skills required to investigate it; for example, the cost of hiring a digital forensics specialist can be high. More importantly, the availability of information will largely affect the cost of an investigation. Organisations should ensure that all required information/documentation is readily available and accessible to investigators in order to reduce both time and costs.

Figure 27 Money spent to investigate economic crime (USD)



Investigating economic crime can be a costly task. By taking a more pro-active approach, such as by establishing a strong ethics and compliance program, organisations can reduce the chances of fraud occurring in the first place – and consequently reduce the likelihood of incurring investigation costs.

Taking it a step further: ethics & compliance

While the rate of economic crime such as accounting fraud, cybercrime, mortgage fraud and tax fraud have increased in the last 24 months, most other types of economic crime have seen a modest drop. This may create a false sense of security and there is a risk that companies may not see the value in investing more resources into business and ethics programmes. However, not to do so would be a strategic miscalculation. In many industries and geographies, risks are not diminishing but are in fact ever-changing and the essence of a successful compliance programme is to proactively anticipate an evolving risk landscape.

To compete at the highest level, today's organisations need to be able to demonstrate that they are committed to embedding ethical behaviour throughout their operations as a key component of corporate strategy. Good policies, procedures and controls are not enough: words need to be backed up by actions, and front-line staff need to have the tools that will help them to live the behaviours that their leaders champion.

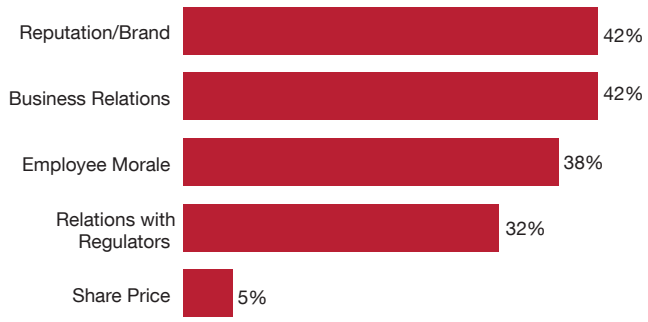
So how does top level management ensure that what they promote is actually being put into practice? Here are four key areas of focus for enhancing the effectiveness of compliance programmes:

- People and culture. Maintaining a values-based programme and measuring and rewarding desired behaviours
- Roles and responsibilities. Ensuring they are correctly aligned with current risks
- High-risk areas. Better implementing and testing
- Technology. Better use of detection and prevention tools, including data analytics

People and culture: your first line of defence

At the heart of any economic crime, irrespective of why it was committed, is a poor decision driven by human behaviour. The solution should therefore begin with people. That means not only instilling clear processes and principles for your employees, but also creating a culture where compliance is hard-wired to values as well as to the overarching strategy of the organisation.

Figure 28 Business operations where fraud impact was significant (Zambia)



While the greatest damage experienced as a result of economic crime is in relation to reputational/brand damage (42%) and business relations (42%), the impact on employee morale (38%) is often overlooked. The truth is, the nature of how a business is perceived – from the inside as well as the outside – should be top management's greatest concern.

In a fast-changing environment, a well-designed compliance programme, supported by a focus on supporting ethical behaviours, can offer a clear strategic benefit to the business. As such, it should include mechanisms to help motivate and reward your people, and to measure outcomes. But to be effective, your compliance programme must comprise more than an updated code of conduct, a policy, and a few hours of training – it must empower your people with an underlying appreciation and understanding of how and why to make the right decisions.

Perception gaps

Nearly all (86%) respondents agreed that their organisation has an ethics and compliance program which set out organisational values and that these values are clearly stated and understood (84%). However our survey identified a number of areas where C-Suite staff were not perceiving the same realities as other staff members.

For example, when asked if rewards are fair and consistent irrespective of level, role, department or location, the majority of C-Suite respondents (71%) agreed with this statement. However, only 43% of all of staff members believe this statement to be true. Although the perception gap is large between C-suite and other staff, one might argue that these two groups will almost never agree on this statement. While issues relating to remuneration will always be a hot topic, disciplinary procedures should be very straightforward and standardised and yet only 55% of staff feel that disciplinary procedures/penalties are consistently applied. Organisations must ensure that unacceptable behaviour is dealt with in a fair and consistent manner if they are to take economic crime seriously.

When asked if senior leaders/managers convey the importance of ethical business conduct in all that they do and thus set a positive example, the gap between C-Suite and other staff is worrisome. While C-Suite respondents agree with this statement strongly (92%), only 62% of other staff members have the same perception of their superiors.

Just over half of other staff members (54%) feel that they are able to raise their concerns confidentially and without fear of retaliation. Should organisations wish for employees to alert potential instances of economic crime, they must create an open environment in which staff feel they can voice their concerns freely and without fear.

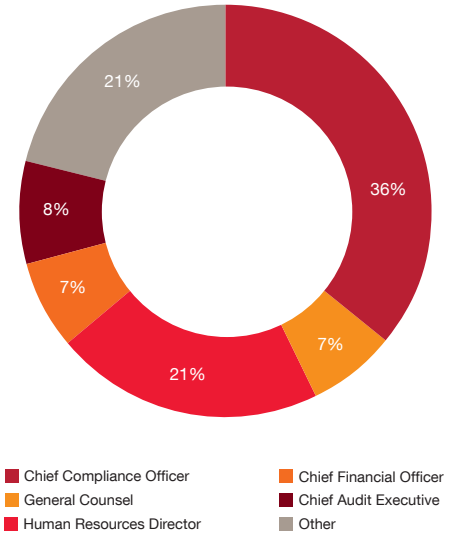
Figure 29 Perception gaps regarding the following statements about ethics and compliance (Zambia)

Gaps between what senior leaders think and say and what lower level staff members perceive can lead to unethical behaviour. Top level management must ensure that these perception gaps are minimized by ensuring what the board believes and promotes is visible to all staff on a daily basis. This is not just the responsibility of the C-suite; there are a number of other key staff members who also have a role to play when it comes to enforcing an ethics and compliance program.

Aligning roles and responsibilities

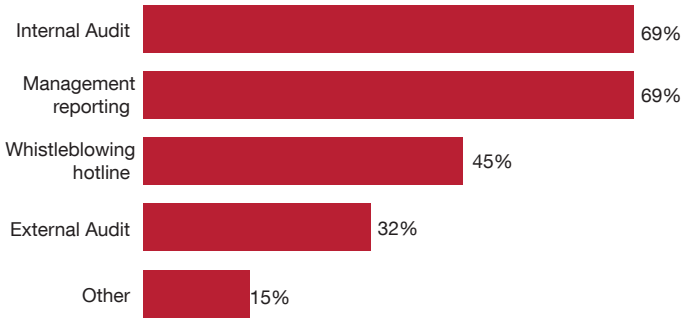
Our survey revealed that 9% of businesses have no formal business ethics and compliance program. Of the 86% of organisations who do have a formal business and ethics compliance programme, responsibility for that programme rests mainly with the Chief Compliance Officer (36%) or Human Resources Director (21%). A further 21% of respondents reported having other individuals responsible for their business and ethics compliance program. These included the Risk and Compliance Manager, the Head of Internal Audit, the Integrity Committee or even individuals on a rotational basis among top managers.

Figure 30 Responsibility for Ethics and Compliance program (Zambia)



While one individual or department may have overall responsibility for the ethics and compliance program, the most effective approach is to ensure that each responsible party (such as those indicated in the diagram above) works together. By ensuring that all take a certain level of responsibility it is more likely that the program will be successfully implemented and maintained. There are a number of avenues through which organisations can ensure their compliance program is effective. Our results show that over two thirds of respondents (69%) are relying on both their internal audit function and management reporting as highlighted in the diagram below:

Figure 31 How do organisations ensure their compliance and business ethics program is effective (Zambia)



This is a good approach as internal audit alone is not a sufficient method of assuring compliance due to the fact that its interventions are both periodic and historical. However by combining internal audits with management reporting and real-time monitoring, economic crime can be detected and prevented in time. Other methods currently being used by our respondents include self-assessments and engaging with law enforcement agencies such as the Anti-Corruption Commission. In any case, in order to enhance the effectiveness of a compliance business ethics program, organisations must ensure that they are aware of certain high-risk areas.

High-risk areas

Ineffective Code of Conduct. Having a recognised code of conduct is crucial, but if employees do not know how to use it in their day to day decision-making then it is not effective. The code and other polices need to be embedded through training, regular communications, reward and recognition (such as when good decisions are made) and disciplinary procedures (when bad decisions are made).

Bribery and Corruption. While 86% of organisations have a code of conduct in place, only 65% of respondents said that training was provided regularly and supported by regular communications and advice channels. Furthermore, while almost all respondents (91%) agreed with the statement that top level management have made it clear that bribery is not a legitimate practice, 45% of respondents feel they are likely to experience bribery and corruption in the next 24 months.

These high risk areas need to be properly monitored and tested through regular training and advice channels if the ethics and compliance program is to be effective and thus prevent economic crime. Technology can also be used as a detection and prevention mechanism through the use of data analytics.

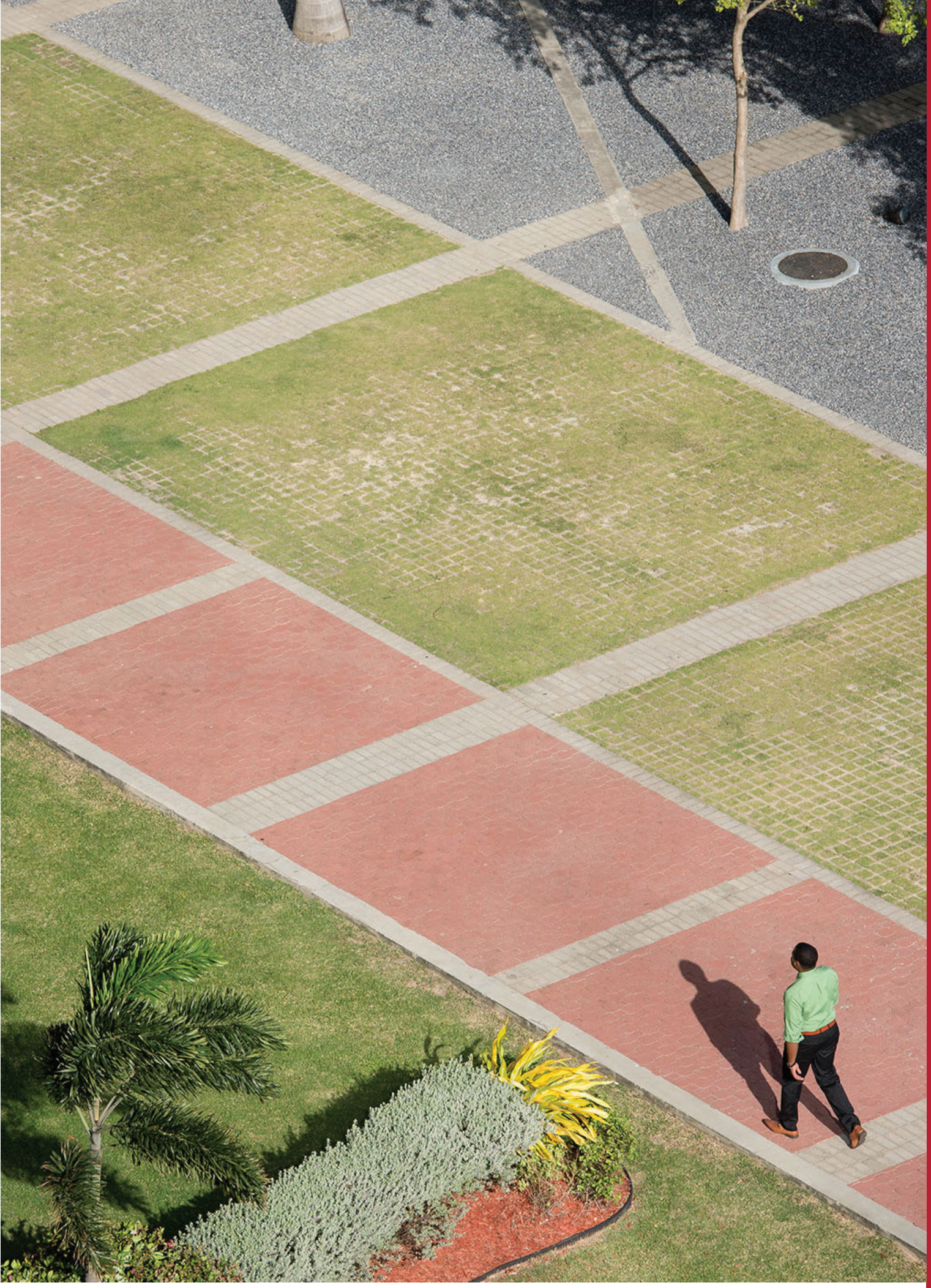
Technology: a powerful tool

Technology can be an effective solution to economic crime, even for companies with limited resources. It is therefore worrying that only 1% of organisations are using this technique to detect economic crime. Data analytics uses a systematic approach to data gathering, cleansing and standardisation. Current technology allows analytics to leverage a growing abundance of available and disparate information and provides a better understanding of both an organisation's data and its potential risks.

A well-designed program should be able to risk-rank transactions and entities for investigation and thus facilitate the detection of hidden relationships and connections with high-risk entities. It should also identify unusual transactional patterns through statistical, keyword and exception-based data mining. The key is to collect data that is both consistent and comparable.

Analytics continues to improve and evolve and companies must ensure that they are leveraging their collective knowledge and experiences from past reviews and investigations in order to maximise the use of data to detect and mitigate fraud. Data is more than numbers: it can serve as a link to crucial insights on trends and behaviours, as well as an early-warning system for areas of potential concern. If used effectively, data can offer companies the additional power to stay ahead of their compliance risks and potentially their competition.

So what makes a company take the leap to new technology? Often such a shift is catalysed by an event such as a remediation due to regulatory sanctions, a merger or acquisition or any other transaction that reveals legacy systems are no longer fit for purpose. Perhaps a new competitor enters the market and changes the stakes for everyone. But sometimes it is simply a matter of an organisation reaching a tipping point when it realises that the expected return on investment of jumping to a new technology platform is greater than the cost of abandoning the systems they have spent millions of dollars on setting up and maintaining.



Conclusion

Our 2016 survey results have brought interesting trends in economic crime to light. These trends can be used to assist you to identify vulnerabilities and accordingly, strengthen processes and develop robust systems to deter, detect and deal with economic crime in your organisation.

In formulating such systems, the engagement and tone of senior management and executives is of paramount importance in their success. These systems need to be constantly evaluated and reviewed in the face of the changing techniques employed by fraudsters and technological advancements. Fraud prevention measures will also be key in acting as a deterrent and in the detection of economic crime.

The shift from the more traditional types of economic crime to the increasing threat of new technologically based crimes indicate that cyber security and an increased monitoring of technological processes should be at the top of agenda for management, for some industries more than others. Top level management must also ensure that an effective and fully functioning ethics and compliance program is put in place in order to minimize internal threats through promoting strong values and corporate behaviour.

Taking a proactive approach to economic crime is critical. Aside from the measurable financial losses, we must take into account the wider impact. This includes the reputational damage and reduced employee morale. It is therefore crucial that organisations focus on the areas they can control by implementing sophisticated measures in order to not only reduce risks, but also deliver business benefits. Given the current state of the Zambian economy and the sharp increase in the rate of economic crime experienced in Zambia, a bold approach to tackling economic crime is not an option – it's an imperative.

Contact us

At PwC, we can carry out fraud risk assessments, cyber security assessments and vendor due diligence to help you identify key risks and threats. Our assessment teams are fast and cost-effective, combining global leading best practices and in-market experience. In addition, we provide investigation services to detect and investigate economic crime. Our regional team of dedicated specialists has conducted a number of complex and high profile investigations undertaken in Zambia and the East Market area in recent years.

Country Senior Partner – PwC Zambia

Nasir Ali
Partner – Zambia
+260 211 334 000
nasir.y.x.ali@zm.pwc.com

Forensic Services Leader

Muniu Thoithi
Forensics Partner, Eastern Africa
+254 (20) 285 5000
muniu.thoithi@ke.pwc.com

PwC Forensic Team

Malvi Chavda
Manager – Forensics
+260 (0) 211 334 000
malvi.chavda@zm.pwc.com

Himonga Michelo
Manager
+260 211 334 000
himonga.m.michelo@zm.pwc.com