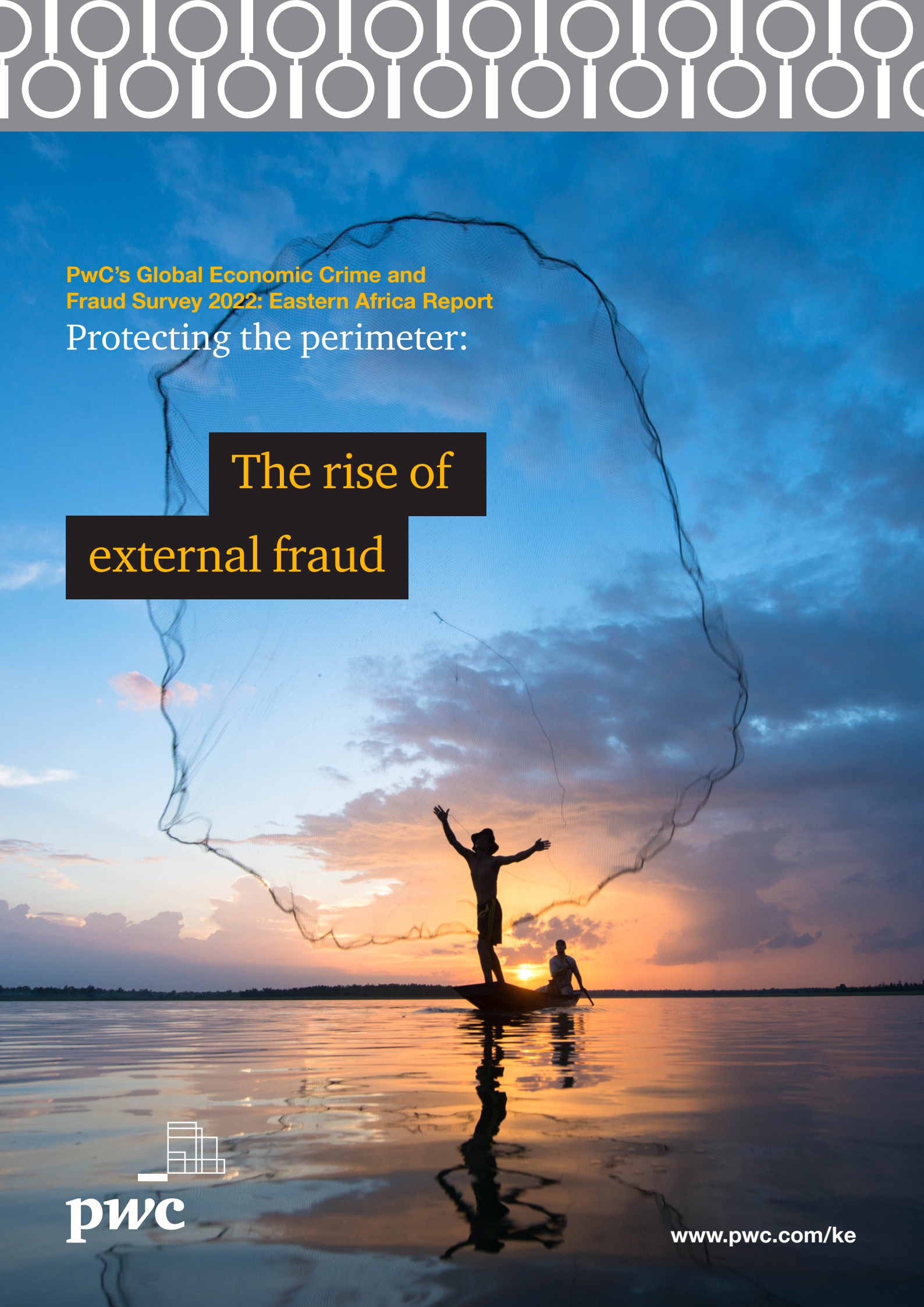


PwC's Global Economic Crime and Fraud Survey 2022: Eastern Africa Report

Protecting the perimeter:

The rise of external fraud

pwc

www.pwc.com/ke

Foreword

Our 2022 Global Economic Crime Survey was performed at a time of significant global change and disruption, driven largely by the COVID-19 pandemic. As well as this, significant progression in areas including technology and ESG have impacted the fraud landscape and created further challenges, resulting in new areas of risk for organisations to navigate. Today's fraud landscape is more complex than ever and presents continually evolving challenges for organisations to contend with.

We have seen economic crime continuing to be an issue to a disproportionate extent in Eastern Africa. A concerning 63% of our Eastern Africa respondents reported having experienced fraud compared to 46% globally.

This discrepancy between Eastern Africa and the rest of the world is continually increasing, with global rates of reported fraud falling over time whilst Eastern Africa results are failing to improve in a sustainable way. We explore potential explanations for this in our report when considering fraud prevention methods in place compared with the most disruptive fraud types in the region.

Unsurprisingly, the shift in management focus and necessity to adapt operational methods during the period of change in which our survey was run opened up new areas of fraud risk and exposure. Increased reliance on technology platforms in operations has simultaneously seen a major increase in cybercrime disruption.

We can also see a significant proportion of crime being committed by internal agents in the Eastern Africa region, reflecting a requirement for improvements in ethical culture which may have weakened during remote working. These results pose the question, are organisations keeping up with developments and focussing on the highest risk areas?

Shifts in the current business climate also bring opportunity in the form of new methods of fraud prevention and detection. New technology tools are creating opportunities for organisations to create genuine value through fraud prevention.

However, just 8% of respondents in the region reported fraud detection through suspicious activity monitoring compared to 13% globally, reflecting a major opportunity to enhance fraud detection. So, how can we enable organisations in the region to embrace these developments?

In our Eastern Africa report we highlight five key themes and areas of insight that are impacting organisations in the region in terms of both risk as well as organisations' responses to economic crime and fraud. These five areas are:

- effectiveness of fraud prevention methods;
- supply chain fraud in an evolving world;
- corruption and accountability in the public sector;
- ESG fraud; and
- cybersecurity risks and exposure.

These areas consider key aspects that organisations can't afford to ignore in the context of the current fraud landscape across the globe.

GECS 2022 survey findings: an overview

2022 saw an increase in the reported incidents of fraud over the 24 month survey period. In this report, we share insights on the types of economic crimes being perpetrated, who is committing the crimes, attitudes towards economic crimes and the steps organisations are taking relating to fraud prevention and detection.

1,296

Global survey of 1,296 executives across 53 countries and regions

63% of Eastern Africa respondents reported having experienced fraud in the past 2 years, compared to **46%** globally

53

countries and regions participated in the survey

62% of the frauds reported by respondents in Eastern Africa were by external perpetrators, either acting alone or colluding with internal actors

Eastern Africa respondents lost a significant amount to fraud in the 2 years covered by the survey

23% reported a total loss of between **$50k to $100k**

23% reported a total loss of between **$100k to $1m**

Top 5 types of fraud reported by Eastern Africa respondents

1. Customer fraud
2. Asset misappropriation
3. Procurement fraud
4. Cybercrime
5. Bribery & corruption and Supply chain fraud

Overview of the 2022 GECS

The 2022 survey considers new types of economic crimes and new forms of old ones

The last half-century has **witnessed a rise in the globalisation of information and finance hitherto unprecedented.** While this has generated innumerable opportunities for organisations to conduct operations from around the world, **it has also spawned a swiftly evolving economic crime environment with new threats and variants emerging every day.**

The increasing variety of economic crime is not the only casualty of globalisation. There is now wide scientific consensus that the **climate is one of the biggest casualties of a highly interconnected and industrialised world.** The business community and particularly regulators have responded by developing Environmental, Social and Governance ("ESG") standards to ensure organisations are acting ethically and sustainably and are not only defining success in traditional profitability metrices but that they are also taking into account the net value they create in or take away from the communities they operate in.

Another consequence of globalisation, particularly coupled with the ubiquity of technology and the social internet, is **the rise of misinformation and disinformation.** This is a key concern not only for individual organisations, but also for governments and multilateral agencies around the world. Coordinated misinformation has permeated through people's daily lives, affecting not just mundane day to day decisions for individuals but collectively influencing, and even swaying, political and consumption preferences for targeted demographics.

A fourth effect of globalisation is that it has **significantly eased the ability for criminals to launder the money derived from illicit activities.** While transnational law enforcement agencies and organisations continue to step up efforts to arrest these

cases, regulations and cooperation varies from country to country, with some countries still having relatively permissive to no money laundering regulations and enforcement.

The year 2019 witnessed a collision course between this rising globalisation and its attendant effects, and the novel Corona Virus disease (COVID-19). Shortly after the World Health Organisation (WHO) declared the virus a global pandemic in March 2020, supply chain operations in many countries ground to a halt. As governments scrambled to procure personal protective equipment, ventilators and later vaccines, conditions that typically heighten opportunities for supply chain fraud were only exacerbated.

The GECS took cognizance of the way these developments impacted the economic crime landscape and has strived to ensure that survey questions stay relevant to the dynamic experience of respondents. As such, the **2022 GECS introduced a number of economic crimes that correspond to these global developments** and that were not covered by previous issues. These include supply chain fraud, disinformation and misinformation fraud, ESG reporting fraud, anti-money laundering, and government relief fraud among others. **This report dedicates a number of sections to covering these new economic crimes as well as some new forms of traditional economic crimes such as asset misappropriation and cybercrime.**

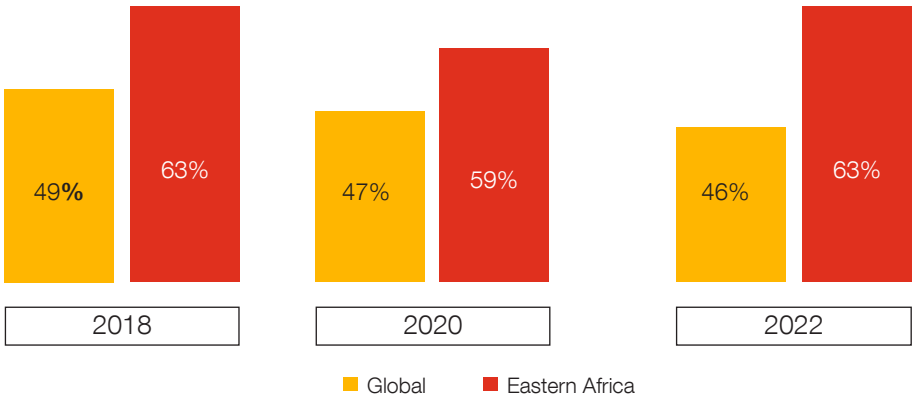
Economic crime remains at a higher prevalence in Eastern Africa compared with the rest of the world

As with every issue of GECS, we asked our respondents whether they had suffered economic crime in their organisations in the last two years. A concerning 63% of our Eastern Africa respondents had experienced fraud within their organisation, against 46% of respondents globally. **This gap is increasing as whilst global reported rates are reducing over time, in Eastern Africa we are seeing rates remain steady.**

63%

A concerning 63% of our Eastern Africa respondents had experienced fraud within their organisation, against 46% of respondents globally

Evolution of reported incident rates in Eastern Africa versus Globally

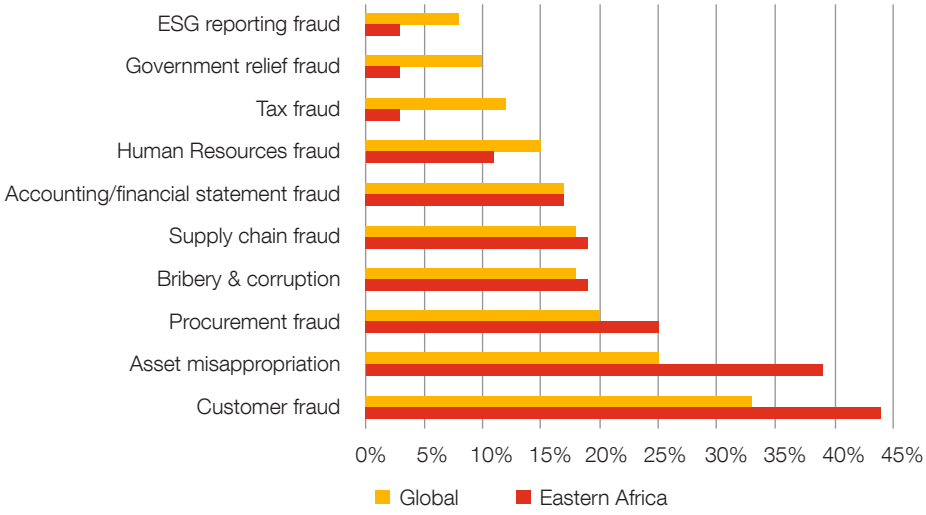


Comparing conduct related economic crime in Eastern Africa vs global incident rate

As shown herein, respondents in the Eastern Africa region reported higher incident rates for more prevalent crimes such as Customer fraud, Asset Misappropriation, Procurement fraud, Bribery & Corruption and Supply Chain fraud.

For less prevalent crimes such as HR fraud, Tax fraud, Government Relief fraud and ESG Reporting fraud, respondents in Eastern Africa generally reported a lower incidence rate than their global counterparts.

This may be in part due to less awareness, for example, relating to ESG fraud, as well as due to a relatively lower level of complexity

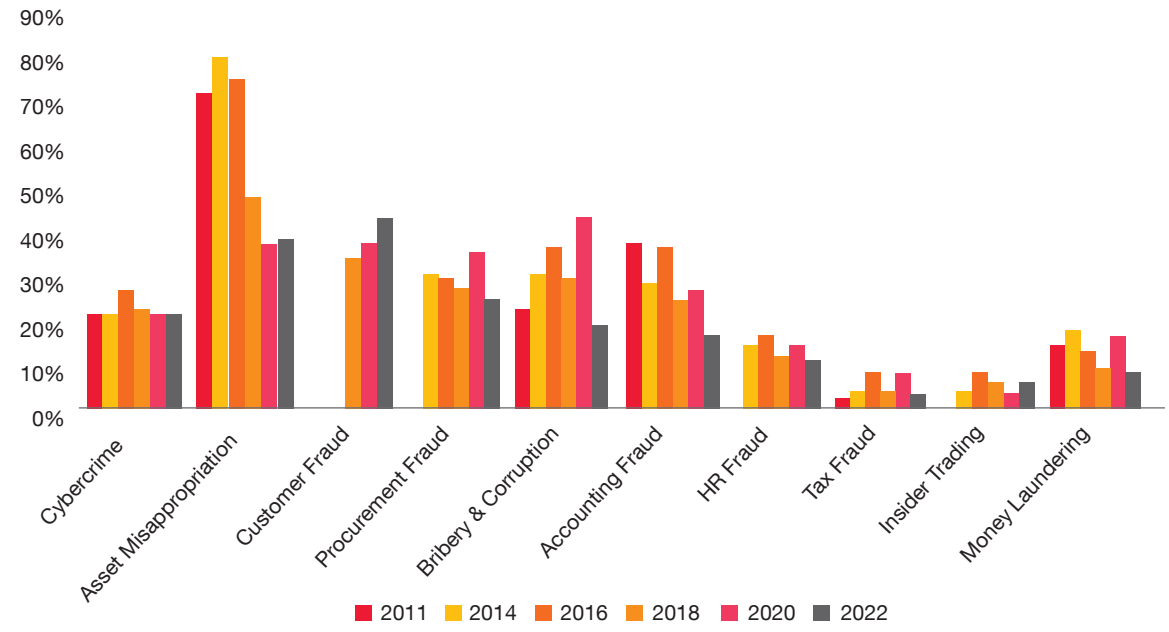


of fraud in the region with the more 'traditional' routes such as procurement and misappropriation remaining prevalent. Although the chart above is limited to types of fraud categorized under conduct risk in the survey, other economic crimes such as cyber crime (22%), money laundering (8%) and insider trading (6%) were also noted as prevalent in the region.

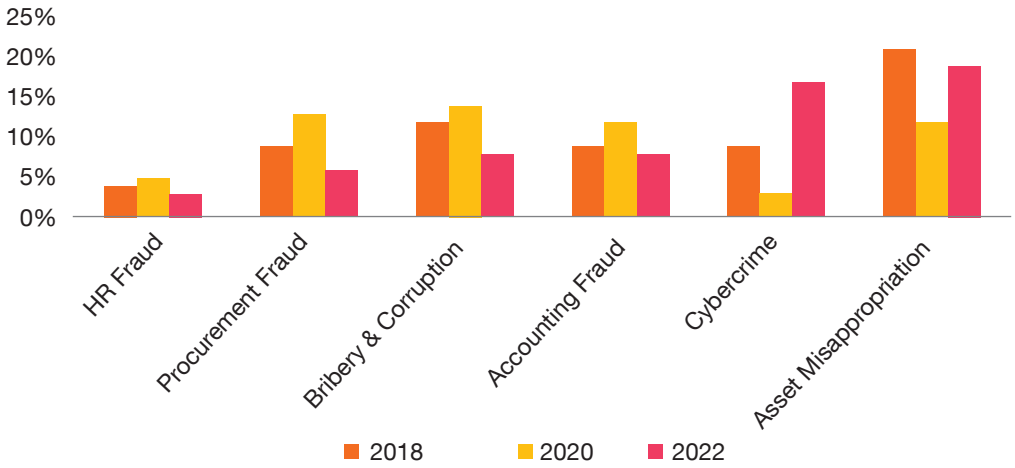
Evolution of economic crime in Eastern Africa over the years

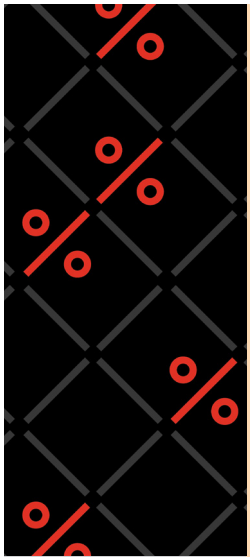
Looking back at the results of GECS for the last 10 years provides an interesting insight into the movement and evolution of economic crime over the years in Eastern Africa.

Movement of key traditional economic crimes over time



The most disruptive economic crimes in the last 6 years





We note the context in which these trends are appearing with relation to the sectoral split of the respondents for Eastern Africa. For instance, the 2022 survey had an increase in the proportion of respondents from the Financial Services industry from 29% in 2020 to 47% in 2022.

At the same time, the 2022 results reflect a reduction in the proportion of respondents from the Industrial Manufacturing sector from 18% in 2020 to 9% in 2022. Whilst many fraud risks typically impact all industries, there are some typologies which are more prevalent in certain sectors. For example, given the increased representation of the Financial Services industry in the survey results, it is not surprising that we are seeing an increase in Cybercrime disruption and Customer fraud.

Financial institutions are a key target and opportunity for cybercriminals. Further, the reduction in reported incidents of Accounting fraud may be partially driven by this being an area which has historically impacted the Industrial Manufacturing industry the most in past survey results.

Based on the graphs above, a few observations can be made from the trend over the years:

- The incidence rate for Cybercrime has not changed significantly over the last 10 years whereas the disruption resulting from these types of fraud has escalated dramatically. Between 2018 and 2022, the proportion of respondents reporting Cybercrime as the most disruptive economic crime has almost doubled, despite reported Cybercrime incidents reducing by 4%. This might suggest that cyber criminals are becoming more targeted, sophisticated and perpetrating fewer but more lucrative cyber-attacks.
- Eastern Africa has been faring well with the majority of economic crime types covered in the survey having seen a decline in reported incidence rate in 2022, other than Customer fraud which has had a significant rise and Asset Misappropriation with a slight increase. The rise in Customer fraud may suggest that organisations paid more effort to prevent internal fraud and may have overlooked rising external threats, suggesting a potential need for a shift in focus in the region.
- There is a declining trend in the number of respondents that reported Accounting Fraud, Bribery & Corruption, Procurement Fraud and HR fraud as being the most disruptive crime in their organisations when 2022 is compared to 2020 and 2018. Bribery & Corruption is at its lowest reported rate since the survey began in the region at 19% of respondents having experienced this in the last 24 months, potentially due to shifting political environments in the region. This could however also point to lower detection rates of some of these economic crimes.

In line with these survey results, we are seeing an evident rise in digital / electronic fraud and Customer fraud in Eastern Africa. From our experience this is being enabled by insiders and technologically savvy customers. Some of the patterns we have identified through our investigations in the region include:

- Complex collusion schemes between staff and customers, enabling mobile banking frauds.
- Over reliance on vendors to support core business operation technology systems.
- Poor or lack of integration of new technologies with legacy systems.
- Insufficient or lack of implementation of system security controls.
- Lack of fraud risk management and monitoring technologies.
- Low fraud incident response readiness.

Impact of COVID-19 on economic crime

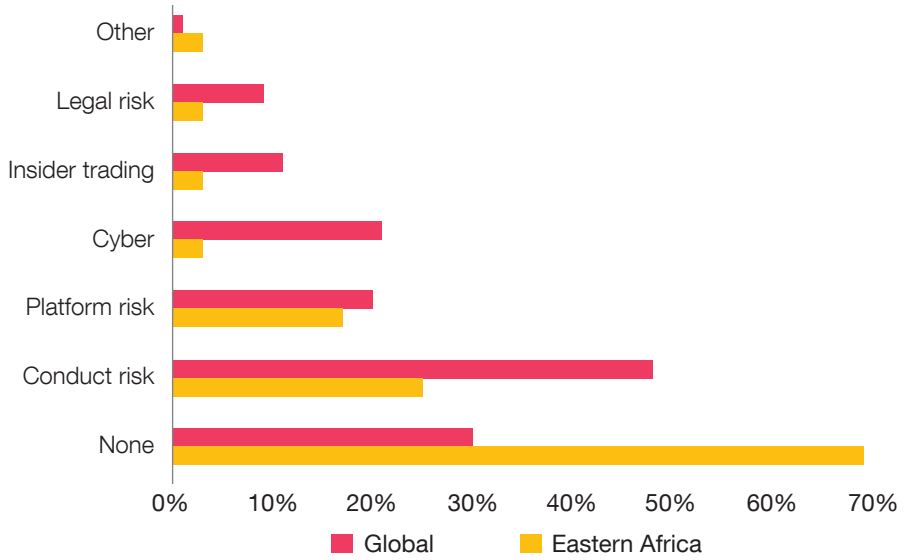
On 11 March 2020, the WHO declared COVID-19 a global pandemic. The disease has become a hallmark event for the turn of the decade, and one of the most disruptive global events for businesses worldwide. COVID-19 has required extensive reorganisation of the nature of work, particularly for businesses that rely on physical office infrastructure, resulting in new opportunities for fraudsters.

For many businesses, digital infrastructure became overwhelmed even as executives and IT personnel scrambled to find ways to increase capacity for remote work. Uncertainty and suppressed spend soon translated to a dip in revenues, requiring reduction in operating expenses. This often meant that critical personnel previously in charge of key control functions, such as risk management, were let go for the survival of the enterprise.

As a result of these gaps, **what may have previously been seemingly innocuous cracks in internal controls became gateways for exploitation by criminals.** This impact was particularly felt globally in 2021 as businesses gradually resumed full operations, and COVID-19 manifested new types of fraud that some businesses had not suffered before as shown in the diagram below:

The rise in Customer fraud may suggest that organisations paid more effort to prevent internal fraud and may have overlooked rising external threats

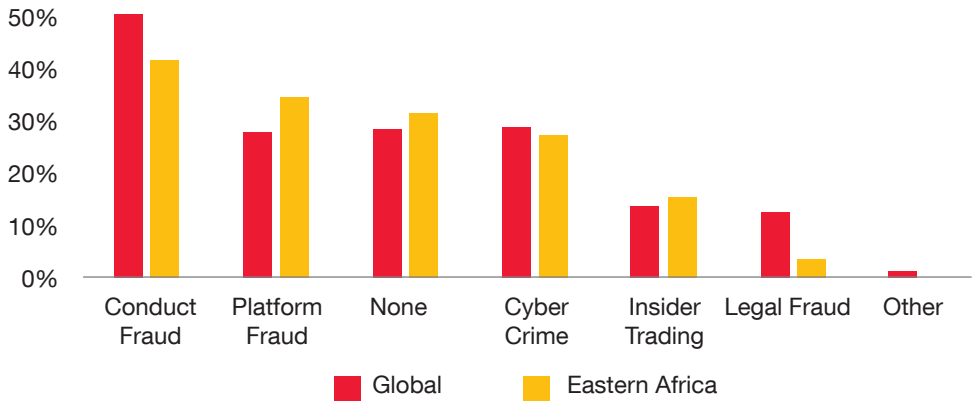
New types of fraud occasioned by COVID-19: Eastern Africa vs Global



A significant 70% of global respondents experienced new types of economic crime which can be attributed to COVID-19. For Eastern Africa, this was less than half, with only **31% of respondents indicating that they had suffered new forms of economic crime as a result of the COVID-19 pandemic.** These reports appear congruent with the WHO global COVID-19 prevalence reports, where Africa is reported to have experienced far less infection incidents than the rest of the world, which would ostensibly translate to less business disruption.

Although this is some reprieve, a significant number of businesses (31%) did experience at least one new type of fraud as a result of COVID-19 in Eastern Africa, with the broader categories of Conduct Risk and Platform Risk being the most prevalent.

Types of fraud with increased risk as a result of COVID-19



Conduct Risk encompasses Customer fraud, Asset Misappropriation, Procurement fraud, and Supply Chain fraud stemming from individual actions. Conversely, Platform Risk refers to the risk of fraud connected to digital platforms that organisations rely on including KYC breaches, Disinformation / Misinformation, Money Laundering and Anti-embargo Trade Violations.

Whilst the rise of reliance on digital platforms enhances efficiencies in key processes, it also increases the inherent Platform Risk faced by organisations.

Interestingly, only 3% of the respondents who reported new types of fraud occasioned by COVID-19 reported to have experienced Cybercrime as a new type of fraud, in comparison to 21% globally. It is noteworthy, however, that 28% of respondents reported experiencing **increased risk** in Cybercrime as a result of the COVID-19 pandemic (in line with 29% globally). This has the implication that although fewer businesses experienced the event of Cybercrime as a new crime because of the pandemic, COVID-19 created fault lines within the organisations that were already vulnerable. These fault lines could be exploited in the future.

31%

31% of Eastern Africa respondents experienced at least one new type of fraud as a result of COVID-19 with the broader categories of Conduct Risk and Platform Risk being the most prevalent'

Whilst the rise of reliance on digital platforms enhances efficiencies in key processes, it also increases the inherent Platform Risk faced by organisations

1

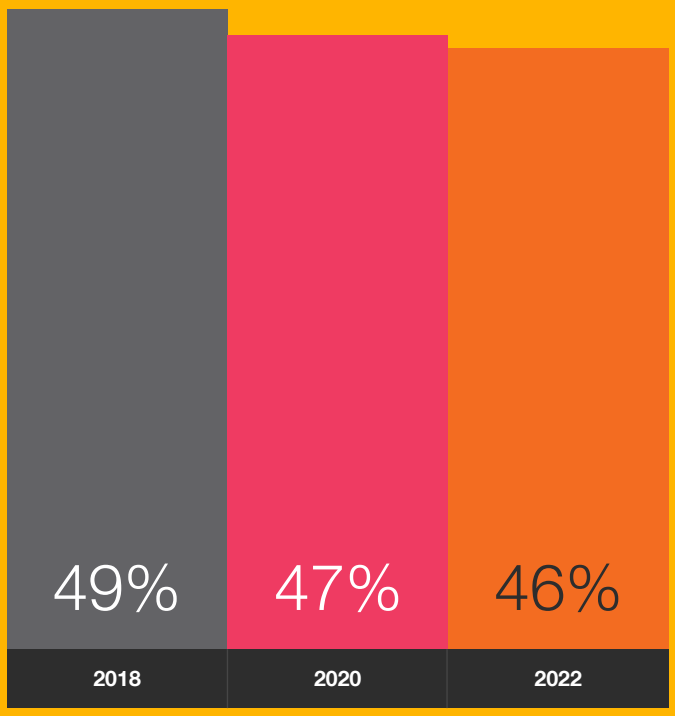
Preventing fraud, have organisations got it right?

Protecting against external perpetrators

The GECS 2022 results show that the percentage of organisations reporting having suffered economic crime globally has remained relatively steady, with only a slight dip over the last three surveys. **This suggests that fraud prevention measures may be working, although more can still be done.**

At a global level, respondents reported that this success has been achieved through the strengthening of internal controls, technical capabilities and reporting. This success has however not been achieved when it comes to managing external fraud, as fraud from external perpetrators acting either alone or in collusion with internal actors has increased both at a global level (45% in 2018 to 69% in 2022) as well as in Eastern Africa (38% in 2018 to 63% in 2022).

Share of organisations experiencing fraud, corruption or other types of economic crime globally



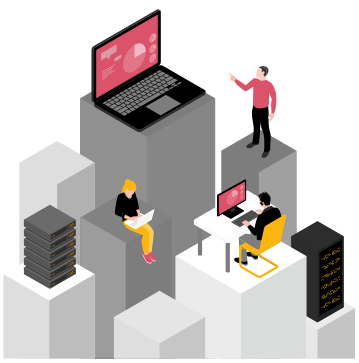
In order to enhance defences against the external perpetrator, organisations should aim to do the following:

1. Understand the end-to-end lifecycle of customer facing products and identify and address opportunities for exploitation that exist.
2. Strike an informed balance between user experience and fraud control.
3. Orchestrate data in a manner that allows for tracking of user activity and generates useful alerts.

The global success in containing economic crime is unfortunately not replicated in the Eastern Africa region with the prevalence rate rising to 63%, moving back towards the 64% reported in 2018 from 58% reported in 2020. This may call for more sustained measures to curb economic crime in the region. Such measures, which need to be deployed consistently and in concert, fall under three areas:

1. Creating a good ethical culture where employees and other stakeholders do not consider economic crime as a reasonable or rational action.
2. Enhanced intervention which encompasses effective detection of economic crime and response.
3. Increased resilience which entails the strengthening of controls making it harder for anyone to perpetrate economic crime.

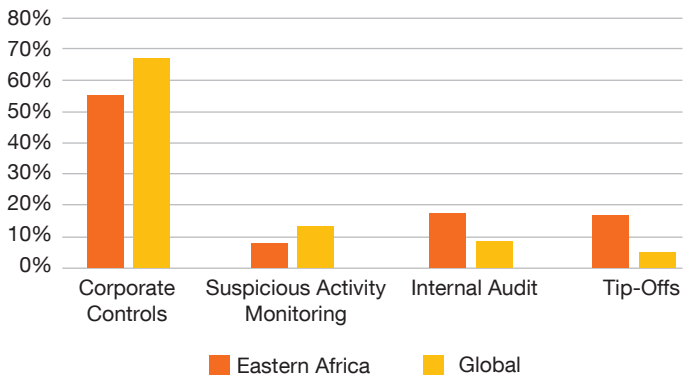
Organisations need to foster the right culture, ensure there are consequences for unethical behaviour and strengthen their anti-fraud controls through implementing strong defences.



The role and effectiveness of various controls in fraud detection

Strengthening controls has the dual advantage of both making it difficult to perpetrate fraud but also assisting in fraud detection.

Controls assisting in fraud detection



Indeed, 58% of respondents in Eastern Africa and 67% globally indicated that they detected their most disruptive fraud through Corporate Controls. Suspicious Activity Monitoring was the most effective corporate control at detecting fraud at 13% globally (8% in Eastern Africa) while Internal Audit at 17% was the most effective in Eastern Africa (9% globally).

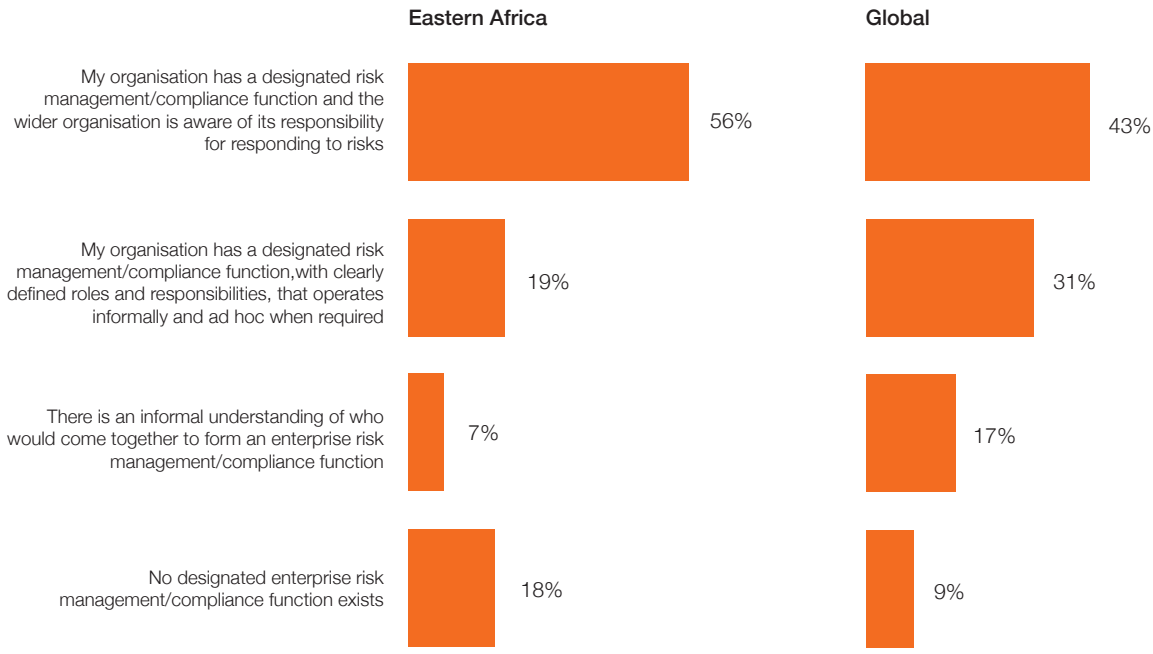
It is worthwhile to note however that tip-offs continue to play an inordinately bigger role in fraud detection in Eastern Africa at 17% as compared to 5% globally. This may point to a need to ensure that whistle-blower channels are implemented and reinforced through culture, employee training and tone from the top. It also points to a likelihood of a big proportion of crimes going undetected as reliance on tip-offs leaves the organisation at the mercy of persons of goodwill and may suggest failure of corporate controls in fraud detection.

As per the survey results, the Eastern Africa region has only a slightly larger proportion of organisations with an Enterprise Risk and Compliance programme that is responsible for responding to fraud risks at 75% compared to 74% globally.

However, these organisations in Eastern Africa have significantly more confidence in the wider organisation's awareness of the compliance / risk function.

Alongside these organisations, the proportion of organisations with no risk management / compliance function is concerningly high at 18% in Eastern Africa compared with just 9% globally. This may be indicative of risk exposure to entities, likely SMEs, that are yet to implement any dedicated compliance / risk management function. This should be addressed as a matter of urgency to guard against the threats of economic crime in today's environment.

Does your organisation have a dedicated Enterprise Risk and/.or Compliance program(s)



The reliance on tip-offs and low use of suspicious activity monitoring reflects discussions we have been having with our clients in recent months.

We have seen clients progressively invest in fraud risk assessments and mapping to ensure deployment of technology and resources is effective and encompassing of the different risks they are facing. For instance, a number of organisations have been enquiring how technology can be leveraged in fraud risk management activities, including prevention and detection.

We hope this reflects a shift in control frameworks and prioritisation of risk management that will assist in protecting local firms, and reduce the gap between the fraud suffered in the region compared to the rest of the world in future survey results.

Leveraging available technology

The use of technology in the Eastern Africa region in monitoring and detecting instances of fraud falls below the global average. Just 8% of respondents reported detection through the means of Suspicious Activity Monitoring compared to 13% globally. Implementing such technology based monitoring processes can provide protection against fraud and economic crime, as potential red flags or issues can be detected earlier, avoiding issues from growing in size and implications.

Technology can assist in the prevention and detection of economic crime in areas such as third party due diligence and ongoing monitoring, ongoing automated transaction monitoring, and compliance monitoring in areas such as conflict of interest / gifts & hospitality for example. The maturity of available technology solutions is continually growing and becoming more sophisticated, resulting in increased accessibility for organisations to embrace the opportunity and implement technology powered approaches to fraud prevention and detection.

The low uptake and use of fraud technology in proactive management of fraud risks can be attributed to a number of factors, including:

- A lack of awareness, understanding and trust of fraud technology and its benefits.
- High initial costs and resource constraints for acquiring the relevant hardware, software, and expertise.
- Outdated or poorly implemented technology infrastructure that limits integration with recent fraud technology solutions.
- A low priority from regulators in enforcing the implementation of fraud technology as a measure of fraud detection.

2

Is Supply Chain fraud hiding in plain sight?

In Eastern Africa, and far beyond, supply chains are going through a phase of unprecedented challenges and transformation. This is fuelled by evolving customer expectations, the need to sustain profitability through cost cutting, a push to meet ESG obligations, disruptions caused by COVID-19, disruptions caused by political instabilities and civil wars, prolonged drought leading to shortage of commodities, and many other intertwined factors.

Organisations have responded to these challenges through interventions such as implementing new monitoring technology, enhanced outsourcing, improved due diligence / onboarding of new partners, venturing to new markets to source for supplies, and other efficiency enhancement related initiatives.

Amid the transformation, the challenges and the ensuing interventions, fraud is emerging as an important issue in the supply chain that has previously not been given the attention it deserves. As organisations invest more time to understand, reorganise and transform their supply chains, they are beginning to appreciate how extensive potential and actual fraud is.

To begin with, they are realising that fraud has been a major cost driver that was hitherto not given the right level of attention. Secondly, they realise that the current environment presents more opportunities for fraud perpetrators to continue engaging in and benefit even more from their fraudulent activities.

54%

Eastern Africa respondents reported a higher incident rate of supply chain fraud at 54% compared to 44% globally

Just over half (54%) of the GECS respondents in Eastern Africa indicated that they have experienced supply chain misconduct in the last two years. This was higher than the global average of 44% highlighting the high prevalence of supply chain misconduct in the region.

About half (51%) of the respondents further informed us that they have experienced misconduct within their third-party suppliers' supply chain, which highlights the fraud risk emanating from third parties and the importance of third-party fraud risk management.

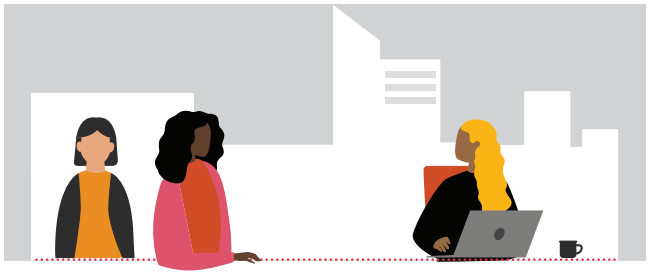
The most common forms of supply chain fraud schemes that the survey respondents cited and that we have seen impacting our clients in Eastern Africa include:

1. procurement malpractices;
2. theft of goods, both internal and external;
3. falsification of transactions and process manipulation by third parties;
4. bribery, kickbacks and extortion by suppliers, intermediaries, government officials etc.;
5. abuse of logistics processes for private benefit; and
6. wastage and avoidable charges which do not fall within the strict definition of fraud but result in avoidable losses by organisations.

Arising from the realisation that fraud is a key supply chain cost driver, we have seen organisations start to take a two-pronged approach when transforming their supply chains, retaining the traditional efficiency centered interventions but also introducing specific interventions to prevent and detect fraudulent activities.

We recently supported a multinational to identify cost savings of upwards of USD 20M from their annual supply chain expenditure following this two-pronged approach. The opportunities for savings were largely from efficiency enhancement, but more importantly from fraud mitigation in their procurement and logistics functions. Specifically on fraud, the cost saving opportunities were from irregular and avoidable spend on technology, freight, warehousing, transport and associated clearing and forwarding services.

In a similar engagement, we assisted an East African diverse automotive sector player realise savings of USD 10M by eliminating irregular clearing and forwarding charges.



Fraud is turning out to be a key supply chain driver and mitigation measures need to be considered in the design of supply chains

Based on our work supporting clients in the region, and the responses that we received during the survey, we note that the underlying factors that contribute the most to supply chain fraud include:

- unfavourable contract terms;
- entrusting supply chain processes to third parties with no proper oversight;
- complexity of the supply chains together with the lack of knowledge by the persons in charge;
- lack of visibility;
- poor planning and budgeting; and
- weak anti-fraud controls.

Based on these observations, it is important for organisations to pay more attention to fraud as they seek to transform their supply chain functions.

Preventing supply chain fraud is a complex challenge. To stay ahead of fraudsters, some of the leading practices that organisations should seek to embrace include conducting regular and proactive fraud risk assessments to understand the nature of fraud risks that they face, the likely impact, their inherent vulnerabilities, and the strength of their controls in deterring fraud.

This will inform among other things the interventions they need to make on their policies, controls, technology, people, and third parties.

3

Corruption and Accountability in the Public Sector

Corruption and accountability are often used interchangeably as interconnected opposites. Transparency International defines corruption as *"the abuse of entrusted power for private gain"* while the Oxford dictionary defines accountability as the act of being *"responsible for your decisions or actions and expected to explain them".*

It is therefore easy to see how corruption and accountability are interconnected. Reduced accountability fosters corruption, and in the viscious cycle, corruption waters down accountability systems, leading to eventual public resignation.

Corruption is an enabler and is often intertwined with other forms of economic crime including Asset Misappropriation and Procurement fraud where rent seekers look to profit illicitly through facilitation fees or kickbacks. Although appearing to slowly decrease over time, we note that Bribery and Corruption, Procurement fraud and Asset Misappropriation continue to be reported among the most disruptive economic crimes with reported incident rates of 19%, 25% and 39% respectively in Eastern Africa.

The anti-corruption formula attributed to renowned professor Robert Klitgaard surmises the relationship between corruption and accountability into a line equation:

Corruption=Monopoly/discretion - Accountability

To fight corruption therefore we should invest in organisational controls that reduce monopoly of information or access / power, and discretion of officers in key processes ("kingpin roles"), while increasing accountability mechanisms.

Countries in the Eastern Africa region have done relatively well in building and strengthening accountability through investments in public finance management (PFM) and in oversight institutions. PFM reforms have sought to improve the planning,

Bribery and corruption incident rates have dropped over time but continue to be reported among the most disruptive economic crimes

budgeting and reporting processes. Oversight institutions include supreme audit institutions, asset recovery agencies and investigative agencies including anti-corruption commissions. These institutions have attracted significant public and donor support, which has been fruitful as we have seen notable successes from them. This includes significant recoveries of unexplained wealth and / or convictions which act as good deterrents to would-be-perpetrators of corruption.

The gains on the accountability front do not however seem to be replicated in respect to the second factor of the corruption equation, being monopoly / discretion. With stretched oversight institutions at the national level, monopoly of information / access as well as power / discretion of officers in key processes has created the opportunity for the various forms of economic crime, especially corruption, to materialise.

For illustration purposes, we look at Procurement fraud in Kenya and Uganda. The respective procurement authorities undertake quarterly market surveys and publish average prices of commonly procured items to guide public procurements. This has however not stopped public sector entities from procuring items at multiple times, sometimes more than tenfold, the average market price. The pertinent question is therefore: at whose discretion are such contracts executed?

More fundamentally, the policies and procedures for fighting corruption appear to all be in place and the gap appears to be how we proactively deal with institutional (could be process specific) "kingpins" who oversee the override of controls. We need to be able to define institution-specific corruption risks, develop mitigating measures and monitor their implementation. Indeed, 58% of respondents in Eastern Africa and 67% globally indicated that they detected their most disruptive fraud through Corporate Controls.

That corruption is still happening and seems to go undetected also means that despite the investments in oversight institutions, there is still room to do more. This includes strengthening areas where notable success has been achieved, such as recovery of illicit wealth, and whistle-blower programmes which facilitate tip-offs which, as earlier observed, continue to play an inordinately bigger role in fraud detection in our region at 17% as compared to 5% globally.

With stretched oversight institutions at the national level, power / discretion of officers in key processes has created the opportunity for the various forms of economic crime, especially corruption, to materialise

4

Are you aware and prepared for ESG fraud?

40% of the survey respondents in Eastern Africa informed us that a general lack of understanding of both what Environmental, Social and Governance ("ESG") considerations mean, and the impact they have to their organisations, are amongst their greatest challenges in managing ESG risks.

In simplified terms, ESG describes non-financial factors that influence the sustainability of an organisation. Environmental factors focus on safeguarding the natural environment which include corporate policies addressing climate change, for example. Social factors focus on how organisations manage matters relating to diversity and inclusion, equity, social justice, and working environments. Governance on the other hand focusses on an organisations' transparency, accountability, and good leadership behaviour etc.

The relationship that exists between sustainable business practices and the achievement of organisational goals is becoming an area of emphasis for stakeholders. Previously, stakeholder decisions heavily relied on financial performance. ESG is now one of the key considerations for many stakeholders. With this increasing importance of ESG, new related risks are emerging, ESG fraud being one of them.

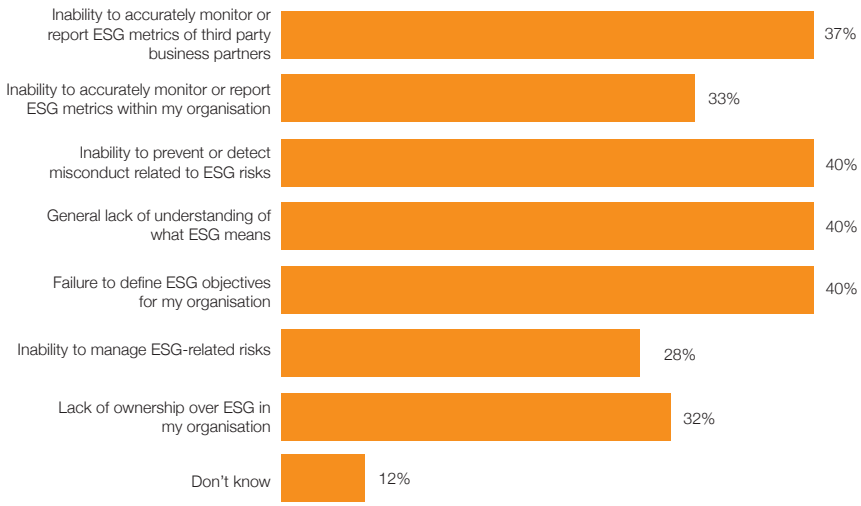
ESG fraud broadly relates to misrepresentation and falsification of ESG factors. The risk of ESG fraud could arise from either within the organisation or through external stakeholders. Examples of internal risk could include misreporting of ESG achievements to meet the expectations of investors, regulators, customers or to meet individuals' performance goals. This is commonly referred to as 'greenwashing'. A more common example of this is bribery of government officials to avoid safety or environmental inspections or to get favourable results. Another form of internal ESG fraud is the manipulation of data to earn ESG credits.

In a project we undertook in the region recently, we observed a potential misrepresentation of ESG project components to stakeholders, resulting in a

misrepresentation of accrued ESG credits to potential customers and investors. As this is an emerging area, the regulatory frameworks are still in the development stage for most countries which, when coupled with the reported limited understanding of the subject, provides an environment in which materialisation of the aforementioned risks can thrive.

External risk exposure on the other hand could be from external stakeholders that organisations interact with, such as customers and service providers. An example of this would be a financial institution funding a customer undertaking a project that is deemed harmful to the environment.

Reported challenges in managing ESG risks



In Eastern Africa, survey respondents indicated to us that the greatest challenges they face in managing ESG risks are:

- a failure to define ESG objectives for the organisation (40%);
- an inability to prevent or detect ESG misconduct (40%); and,
- a general lack of understanding (40%).

ESG fraud could lead to serious consequences for an organisation, its executives and business partners. The most fundamental being failure to achieve organisation goals for not embracing sustainable business practices. Others could include reputational damage, fines, and penalties.

This reinforces the need for organisations to be aware of ESG fraud as an emerging form of economic crime as they continue to embed ESG practices into their business operations. It is important for organisations to put in place ESG fraud mitigating measures from the onset at the core of their ESG strategy. It pays to proactively get it right from the onset instead of dealing with the aftermath. This can be achieved through raising awareness, conducting risk assessments, and embedding ESG fraud management within the established risk management practices.

It is also instructive to note that in getting the 'Governance' pillar right, organisations will have created and fostered an environment that allows them to effectively manage the risk of fraud and other economic crimes.

5

Cyber Security

The COVID-19 pandemic had a significant impact on the global economy, disrupted businesses and forced most businesses that could digitize to do so. Some organisations also moved to outsourcing managed services to cope with the increasing strain on limited resources.

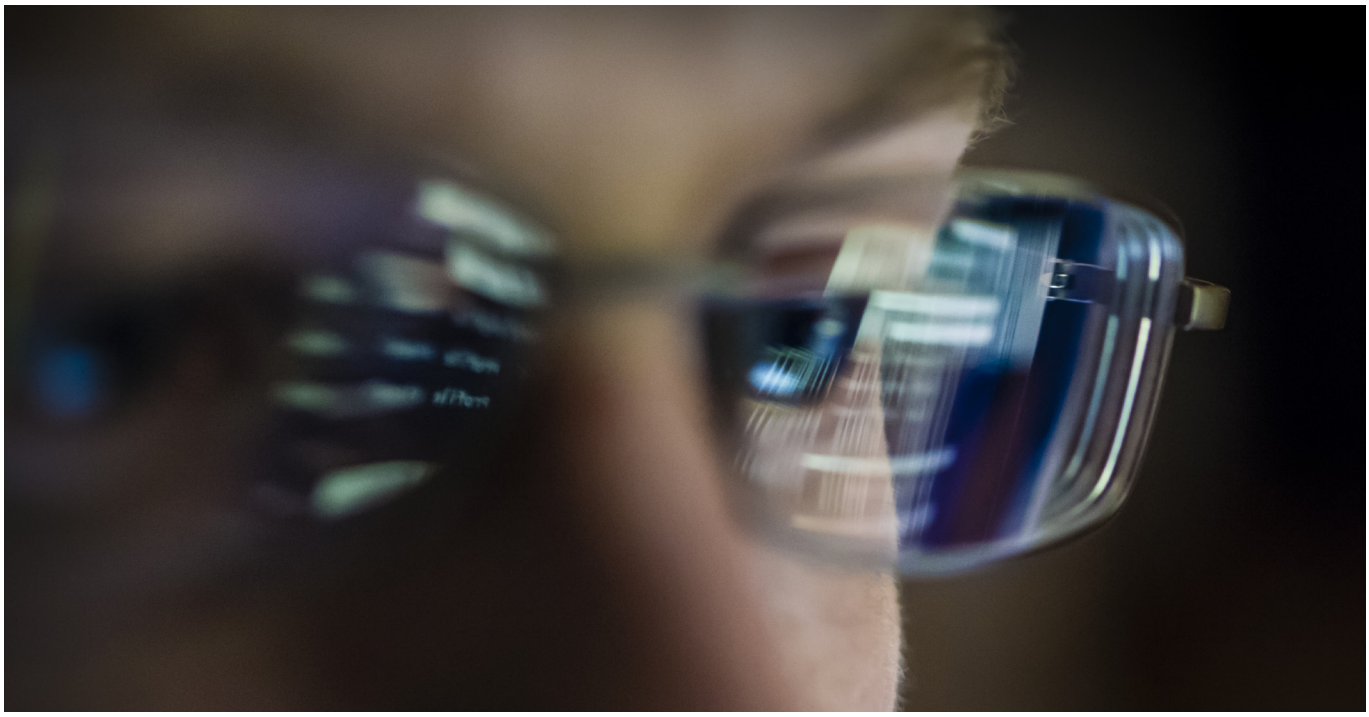
The economic and social disruptions led to changes in human behaviour, new ways of using technology and novel opportunities to do business. Many businesses were forced to transform rapidly to support remote working, which increased their reliance on hastily deployed Virtual Private Networks ("VPNs") and remote administration technologies. The rapid transitions to remote work put pressure on IT security teams to understand and address a wave of potential IT-related security risks in a short space of time. Some organisations reduced the number of their IT security staff in response to economic challenges, depleting their cyber intelligence and threat monitoring capabilities and compounding the risks.

28%

of respondents reported experiencing increased risk in Cybercrime as a result of the COVID-19 pandemic

There was an expectation that the surge in electronic communications for business interactions would provide an opportunity for cybercriminals to target organisations through the use of phishing schemes and click bait. As expected, the use of malicious emails and websites did become increasingly prevalent as the volume of emails from employers, governments, security and health agencies was at a record high.

Further, technology developments such as the rise of AI, for example Chat GPT, has made phishing fraud more accessible to criminals and compounded the risks. The data reflects this when we consider reported cybercrime incidence falling yet it being reported as



the most disruptive economic crime globally. **Cyber criminals are becoming more sophisticated and perpetrating fewer but more lucrative cyber-attacks.**

COVID-19 accelerated the use of technology platforms within organisations' operations such as customer management systems, social media platforms and third-party monitoring systems, especially in SMEs.

This has created new aspects of risks for organisations to understand and manage if they are to guard against potentially significant financial, reputational and regulatory damage created by cybercrime.

In Eastern Africa, 28% of respondents confirmed that there was an increase in cyber risks in their organisations because of disruption caused by the COVID-19 pandemic. They however were cognizant of the fact that cybercrime is not new and was not initiated by COVID-19.

However, despite the increased risk being recognised by respondents, the expected rise of cybercrime was not evidenced in the results in Eastern Africa. In Eastern Africa 22% of the respondents reported having encountered instances of cybercrime compared with 23% and 22% in 2018 and 2020 respectively.

This steady trend shows that cybercrime remains a significant area for organisations to focus on, and that the heightened risk reported likely resulted in additional controls which have worked in keeping reported cybercrime incident rates steady.

Detection and prevention methods

Detection and prevention of cyber related fraud requires implementation of multiple techniques that combine technology, processes, and people.

Some of the strategies that individuals and organisations can deploy to protect their assets from cyber threats include:

- Security Awareness and Skills training

- Data Protection and Data Loss Prevention
- Identity and Access Management (System level and physical).
- Continuous Vulnerability Management
- Network Monitoring and Defence, Inventory and control of Enterprise and Software assets
- Incident Response Management

Means by which cybercrime activities were initially detected:

76%	15%	6%	3%
corporate controls	influence of management	corporate culture	Other mechanisms

The above chart shows that corporate controls are key in detection of cybercrime, and that robust internal controls are critical in ensuring that cybercrime fraud is identified quickly, preventing the issue from remaining undetected and growing significantly.

Profile of cybercrime fraudsters

of which

65%	68%	39%
External actors	Hackers	Organised crime groups

The above highlights the requirement for sophisticated prevention methods to defend against these professional perpetrators.

These individuals are sophisticated and invest time in continuously updating their *modus operandi,* enabling them to adapt their methods to the enhanced measures organisations are implementing. No organisation can afford to stay still when it comes to their cybercrime controls.

6

Conclusion – key takeaways for protecting your perimeter

Our report has highlighted and evidenced that today's fraud landscape is more complex than ever and presents continually evolving challenges for organisations to contend with.

It can become overwhelming to consider the various threats your organisation faces and to keep up with the pace of change, but we have seen that it pays to have an ongoing focus on your fraud risks and controls.

Fraud risk evolves with the evolution of the business environment, in response to emerging areas such as the current focus on ESG and increased digitisation of supply chains, and in reaction to internal control measures. As such, continuous risk management is important to mitigate emergence of new types of economic crimes or evolution of existing typologies.

We have highlighted the below as key areas for focus in the region based on the results of our survey:

- **Use of technology:** Eastern African respondents reported less use of technology tools such as automated suspicious activity monitoring for fraud prevention which presents a major opportunity for improvement.
- **Reinforcing whistle-blower channels:** As observed, tip-offs continue to play an inordinately bigger role in fraud detection in Eastern Africa at 17% as compared to 5% globally. There is an opportunity to enhance this further by ensuring that whistle-blower channels are implemented and reinforced through culture, employee training and tone from the top.
- **Continuous evaluation of fraud risk management programmes:** Given the rate of evolution of the current fraud landscape, maintaining ongoing oversight of your fraud risk management programme is critical. Ensuring the programme is designed with the flexibility to adapt as needed when new risks emerge is key in protecting your perimeter and ensuring that the controls in place are fit for purpose at any given point in time. Regular fraud risk assessments and controls evaluations are key in this.

PwC Eastern Africa Forensics leadership and management team

Muniu Thoithi
Advisory & Forensics
Leader, Eastern Africa

muniu.thoithi@pwc.com
+254 722 292 012

George Weru
Partner,
Forensic Services

george.weru@pwc.com
+254 727 341 584

John Kamau
Associate Director,
Forensic Services

john.kamau@pwc.com
+254 701 849 039

Patrick Matu
Associate Director, Forensic
Services

patrick.k.matu@pwc.com
+256 761 507 789

Chrisantus Khulabe
Senior Manager, Forensic Services,
Digital Forensics & Data Analytics lead

chrisantus.khulabe@pwc.com
+254 758 726 206

Titus Kariuki
Senior Manager, Forensic Services
Financial Services lead

titus.kariuki@pwc.com
+254 726 898 699

Johnstone Mwendwa
Manager, Forensic Services

johnstone.mwendwa@pwc.com
+254 110 633 491

Brenda Guchu
Manager, Forensic Services

brenda.guchu@pwc.com
+254 110 633 490

Hazel Woodhead
Manager, Forensic Services

hazel.w.woodhead@pwc.com
+254 797 379 606

At PwC Eastern Africa, we are a multi disciplinary team of over 25 forensic specialists that serve public and private sector clients in Kenya, Uganda, Tanzania, Zambia, Rwanda and Ethiopia. We carry out fraud risk assessments and cyber security assessments to help you identify key risks and threats, as well as providing litigation support when needed. Our assessment teams are fast and cost-effective, combining global leading practices and in-market experience.

In addition, we provide swift and effective responses through our investigation services to detect and elucidate economic crime and enhance our clients' resilience.

Our regional team of dedicated specialists has conducted some of the most complex and high profile investigations undertaken in Eastern Africa in recent years.

Contacts

Kenya & Ethiopia

Muniu Thoithi
Advisory & Forensics Leader,
Eastern Africa

muniu.thoithi@pwc.com
+254 722 292 012

George Weru
Partner, Forensic Services
PwC Kenya

george.weru@pwc.com
+254 727 341 584

John Kamau
Associate Director,
Forensic Services
PwC Kenya

john.kamau@pwc.com
+254 701 849 039

Uganda

Uthman Mayanja
Country Senior Partner
PwC Uganda

uthman.mayanja@pwc.com
+256 312 354 400

Patrick Matu
Associate Director,
Forensic Services
PwC Uganda & Rwanda

patrick.k.matu@pwc.com
+256 761 507 789

Rwanda

Moses Nyabanda
Country Senior Partner
PwC Rwanda

moses.o.nyabanda@pwc.com
+250 252 58820

Tanzania

David Tarimo
Country Senior Partner
PwC Tanzania

david.tarimo@pwc.com
+255 754 784 844

Chacha Winani
Associate Director,
PwC Tanzania

chacha.winani@pwc.com
+255 756 223 377

Zambia

Andrew Chibuye
Country Senior Partner
PwC Zambia

andrew.chibuye@pwc.com
+260 761 835 505

Moonga Hamakule
Senior Manager,
PwC Zambia

moonga.hamakule@pwc.com
+260 973 084 748

www.pwc.com/ke