



Fraud, Financial Reporting and the Role of the Auditor – The IRBA Indaba

Webinar: 6 August 2024

Agenda

#	Item	Time	Presenter
---	------	------	-----------

Welcome and Introductions (10 min)

Fraud Landscape (1.15 hours)

1.	Emerging Fraud Trends	13:10 – 13:35	Greg Truter
2	Fraud Risk Management Frameworks and Tools	13:35 – 14:00	Manuel Caldeira
3	Cybersecurity, Financial Reporting and Audit	14:00 - 14:25	Lucien Pierce

Q&A (10 minutes)

Comfort Break (10 min)

Fraud in Practice (50 minutes)

4	Employee Fraud	14:45 – 15:10	Abdullah Seedat
5	Conversation with a whistleblower	15:10 – 15:35	Ronèl van Wyk & Runya Makanza

Q&A (10 min)

Webinar Conclusion (5 min)

Fraud Landscape 1 : Emerging Fraud Trends presented by Greg Truter



Position: PwC Partner in forensic services.

Experience: Over 22 years of experience, specialising in forensic investigations, accounting litigation support, alternative dispute resolution, claim reviews and preparation.

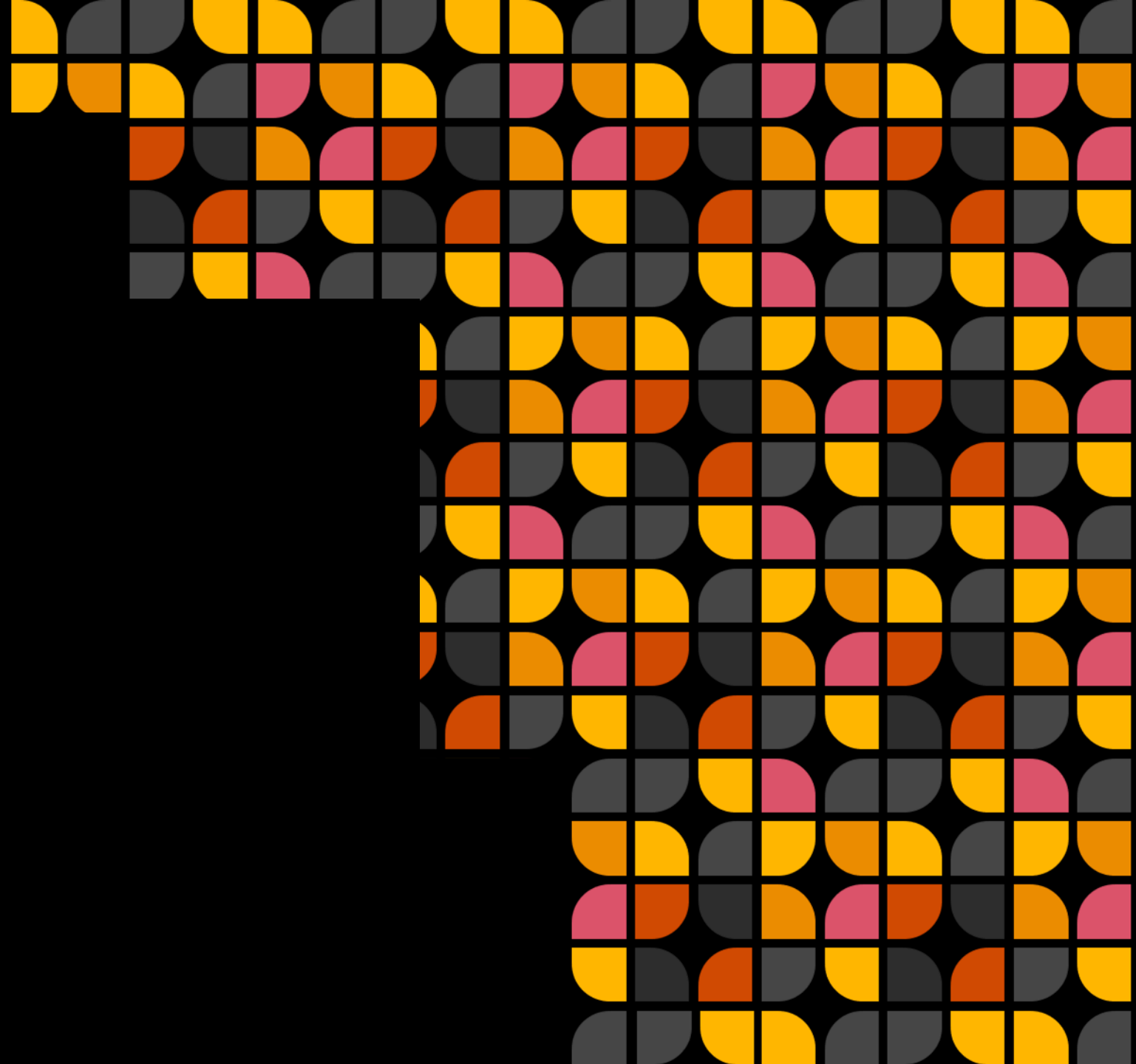
Qualifications: CA(SA), Registered Auditor, and Commercial Forensic Practitioner.

Client Base: His experience spans from large multinational corporate entities and public sector clients to smaller family-run businesses.

Global Perspective: Greg's involvement in multiple high-profile matters allows him to bring a global perspective to his broad client base.

Emerging Fraud Trends

The IRBA Indaba
6 August 2024





Fraud, the ever-present risk

By the numbers	1
Not all fraud is equal	2
Not all fraud has an equal impact	3
What do we do about it?	4



By the numbers

Leading Practice Interviews

1 Fraud: 55% report that procurement fraud is a widespread concern in their country, yet a minority are using available tools to identify or combat it. Nearly 20% do not use data analytics in any way to identify procurement fraud, and just 26% are leveraging data analytics to identify unusual bid patterns

2 Corruption: 81% believe government efforts to enforce anti-corruption laws are becoming more robust or remaining steady in the countries in which they operate. While 77% are confident their compliance programmes can mitigate emerging risks, it is worrying that 42% of companies either don't have a third-party risk management programme or don't do any form of risk scoring as part of their programme.



In all its forms, fraud remains a persistent challenge.

Source: PwC's Global Economic Crime Survey 2024



Q1. Percentage of organisations experiencing economic crime over the last 24 months

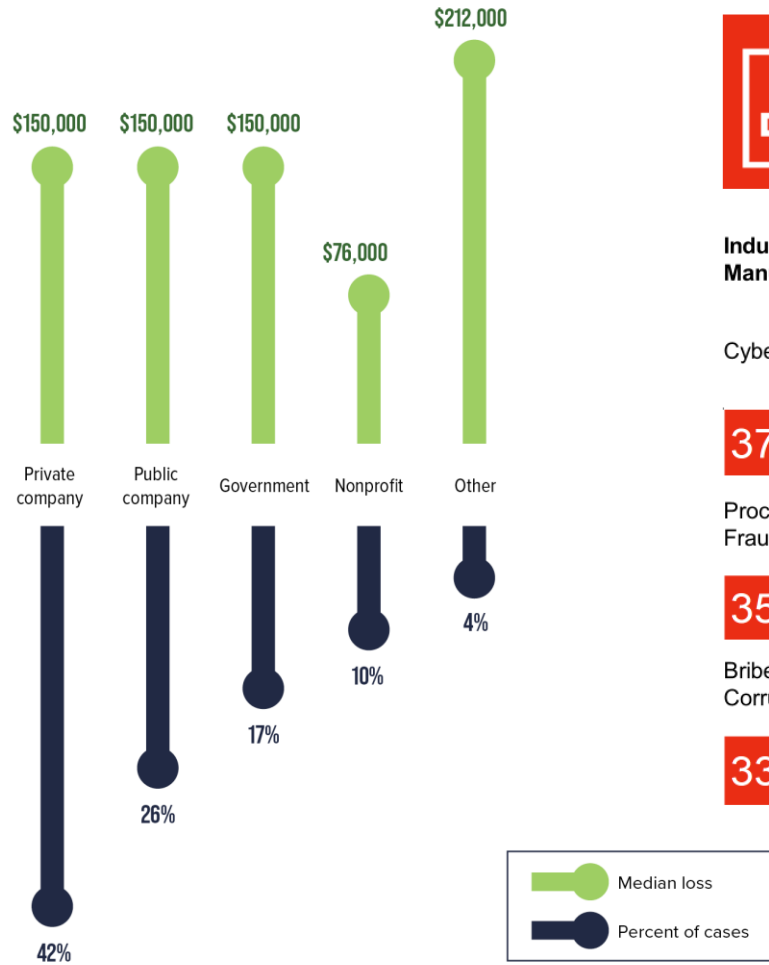
41% Global

46% Africa

Where is this happening?



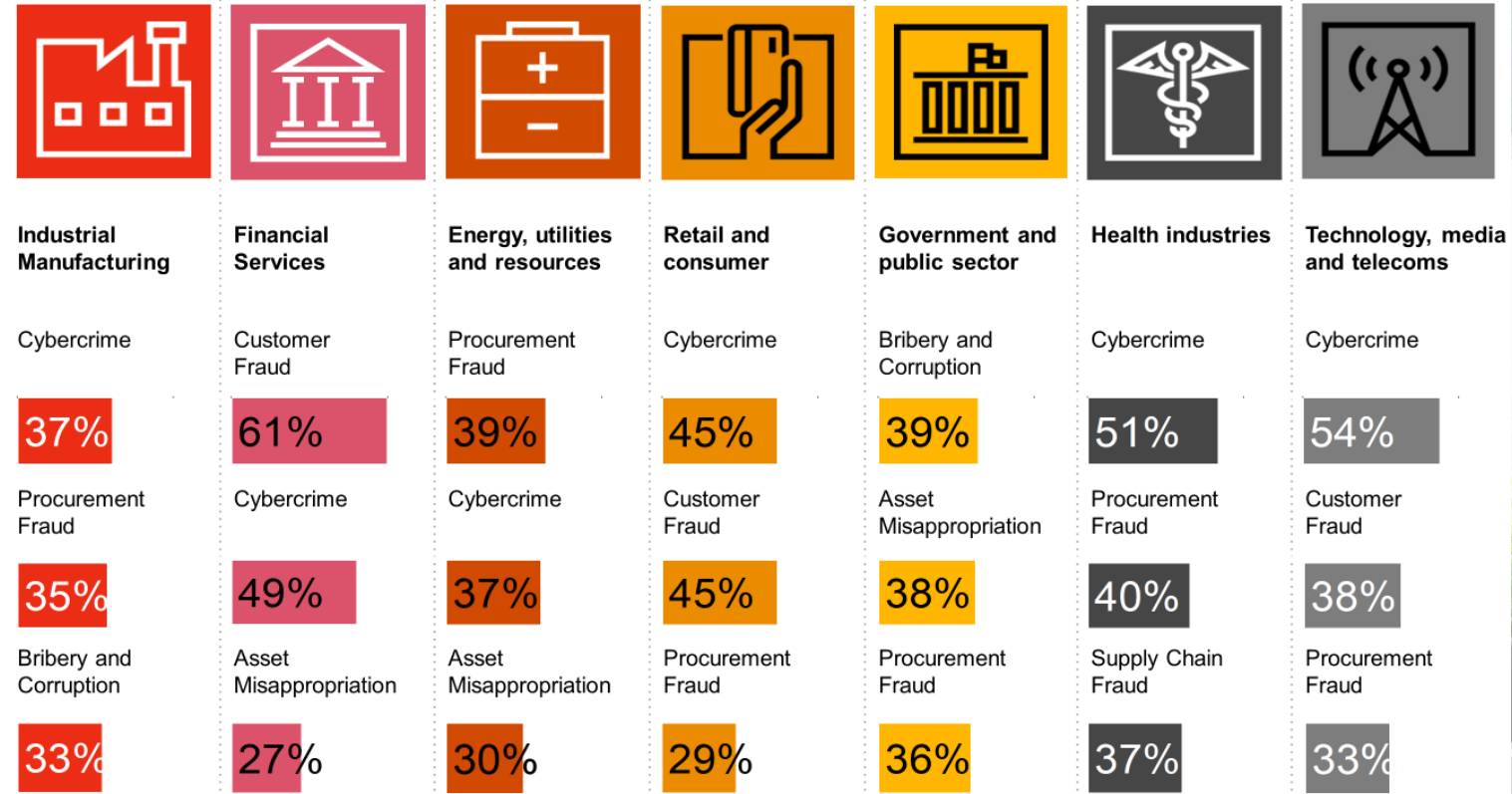
FIG. 20 WHAT TYPES OF ORGANIZATIONS ARE VICTIMIZED BY OCCUPATIONAL FRAUD?



Source: ACFE 2024 Global Report to the Nations

Types of fraud experienced, by industry

Source: PwC's Global Economic Crime Survey 2024





2

Not all fraud is equal

What is happening?



FIG. 97 WHAT ARE THE MOST COMMON OCCUPATIONAL FRAUD SCHEMES IN SUB-SAHARAN AFRICA?

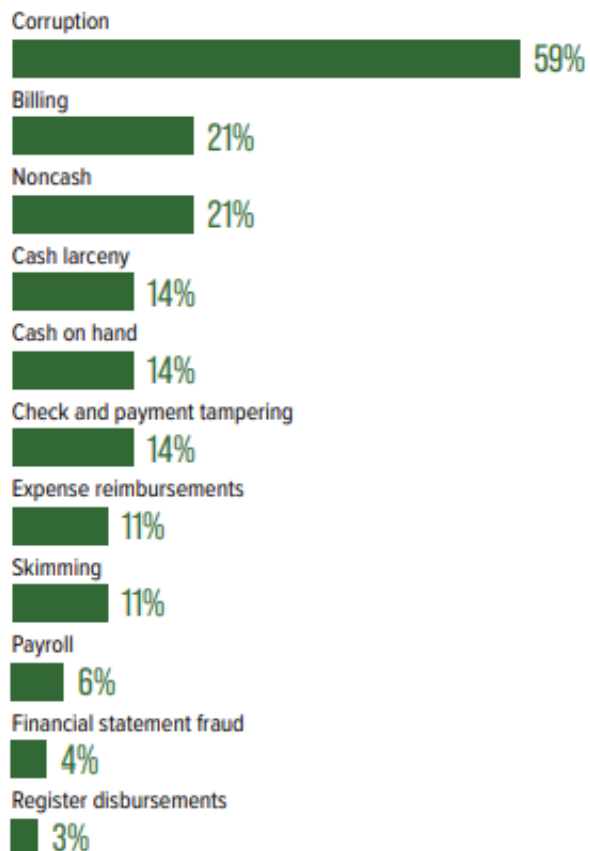


FIG. 98 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED IN SUB-SAHARAN AFRICA?

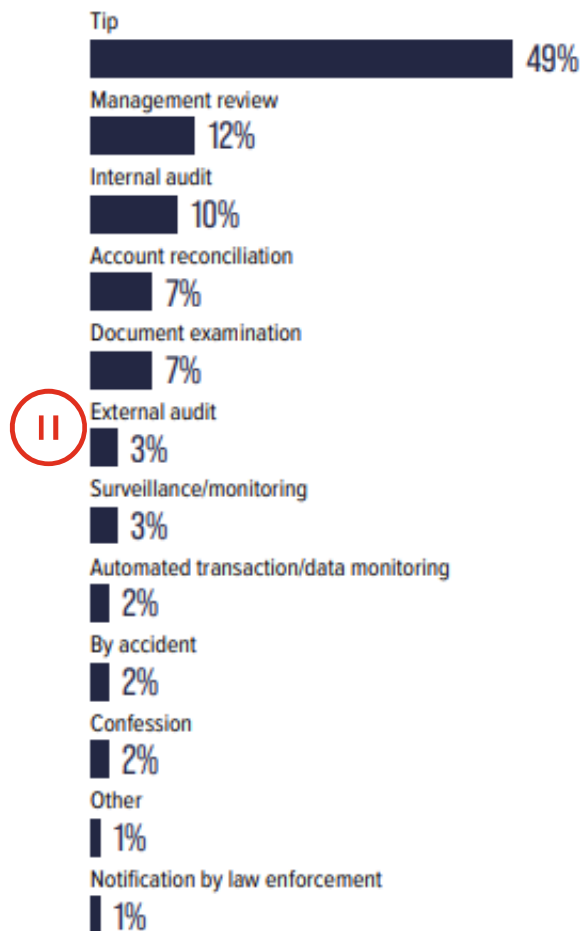


FIG. 99 WHAT ANTI-FRAUD CONTROLS ARE THE MOST COMMON IN SUB-SAHARAN AFRICA?

Control	Percent of cases
External audit of financial statements	90%
Internal audit department	88%
Code of conduct	85%
Management certification of financial statements	82%
External audit of internal controls over financial reporting	74%
Independent audit committee	73%
Hotline	70%
Management review	67%
Anti-fraud policy	63%
Fraud training for employees	63%
Fraud training for managers/executives	60%
Dedicated fraud department, function, or team	53%
Employee support programs	50%
Formal fraud risk assessments	47%
Surprise audits	44%
Proactive data monitoring/analysis	39%
Job rotation/mandatory vacation	23%
Rewards for whistleblowers	13%

Source: ACFE 2024 Global Report to the Nations



What is happening?

FIG. 97 WHAT ARE THE MOST COMMON OCCUPATIONAL FRAUD SCHEMES IN SUB-SAHARAN AFRICA?

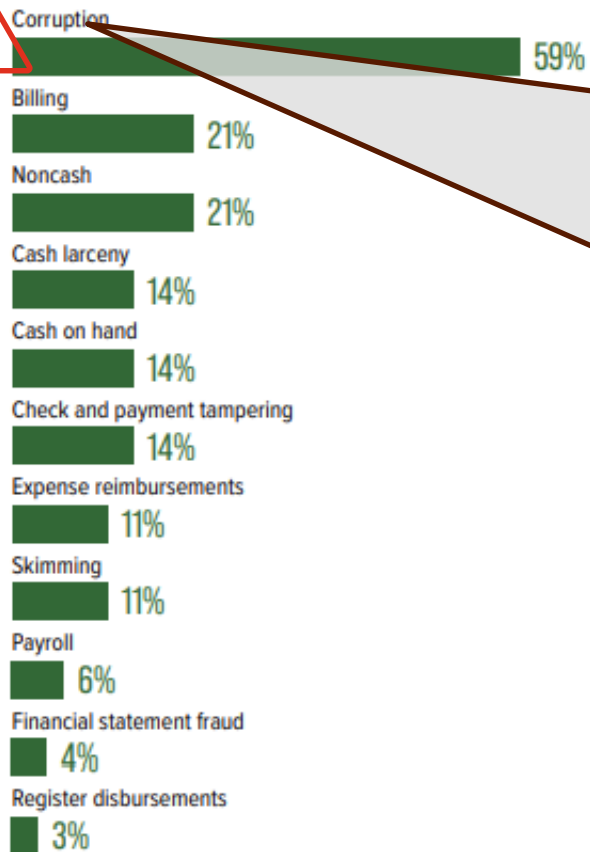
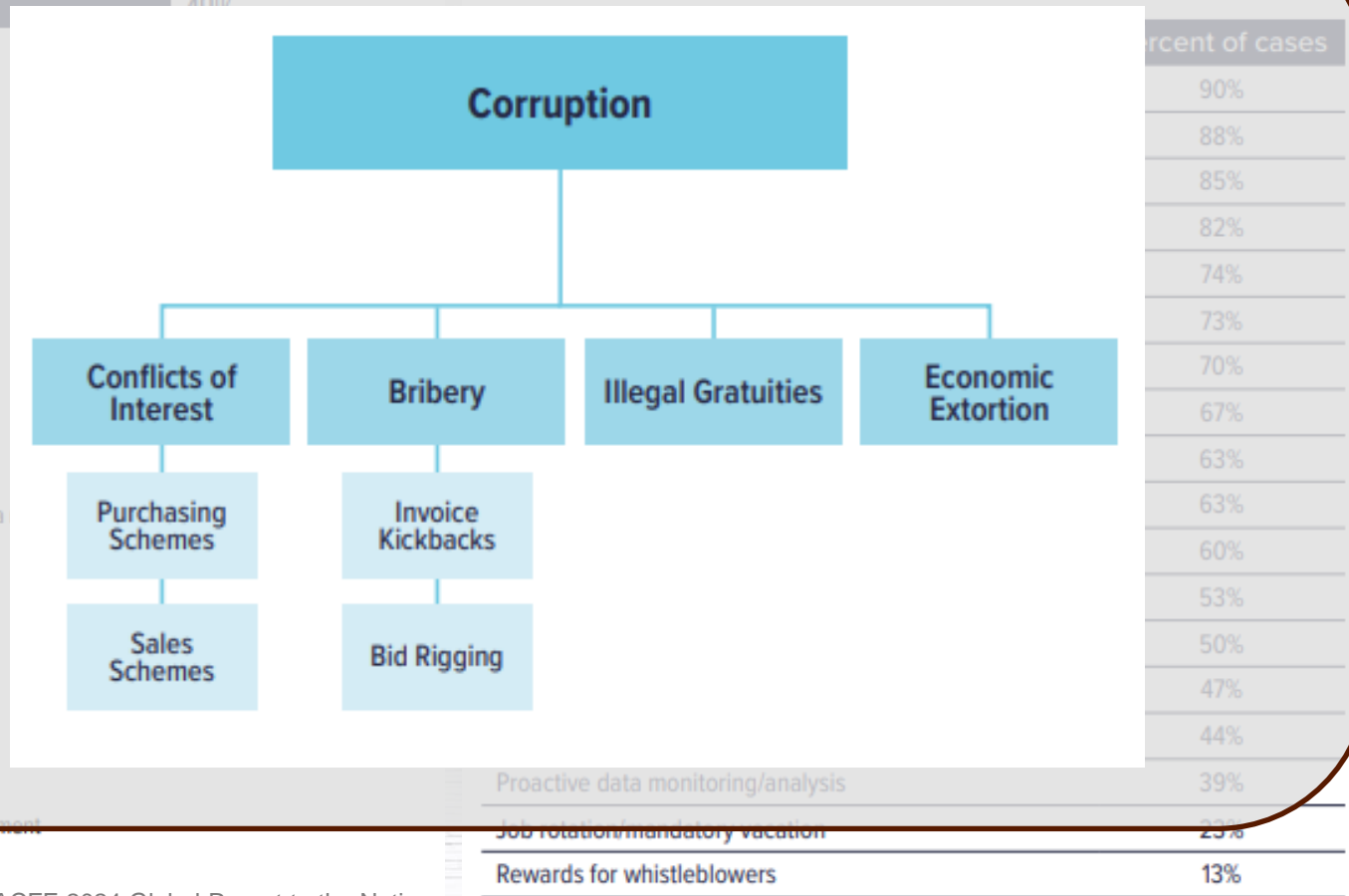


FIG. 98 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED IN SUB-SAHARAN AFRICA?



FIG. 99 WHAT ANTI-FRAUD CONTROLS ARE THE MOST COMMON IN SUB-SAHARAN AFRICA?



Source: ACFE 2024 Global Report to the Nations



What is happening?

Q3. What types of fraud, corruption or other economic crime has your organization experienced in the last 24 months?



Material: qualitative / quantitative
Non-compliance: direct / indirect



What is happening?

PwC's Global Economic Crime Survey 2024



Economic crime risk is more complex than ever before—and it is far more challenging to both create value and protect it.

In parallel, governments around the world are signalling their rising expectations that companies do their part to prevent economic crime and more fully disclose its consequences.

Risks are inevitable. It's whether a company takes, and mitigates, risks intelligently to grow and thrive that sets leaders apart.

In today's global, interconnected environment, economic crime is a pervasive challenge. Geopolitical pressures heighten sanctions and export controls risks. Exposure to bribery and corruption risks expands as global companies enter new markets in search of growth. There is increased public and regulatory scrutiny regarding use of forced labour and other environmental, social and governance (ESG) responsibilities—not just in companies but anywhere in the supply chains that support them. And, as the mergers and acquisitions market strengthens, acquirers can be exposed to potential liabilities associated with illegal acts hidden in their new assets. Economic crime risk is more complex than ever before—and it is far more challenging to both create value and protect it.

In parallel, governments around the world are signalling their rising expectations that companies do their part to prevent economic crime and more fully disclose its consequences. Regulatory enforcement and cross-border cooperation amongst law enforcement agencies are increasing in an effort to combat bad actors and the devastating impact their actions can have on individuals, businesses and economies.

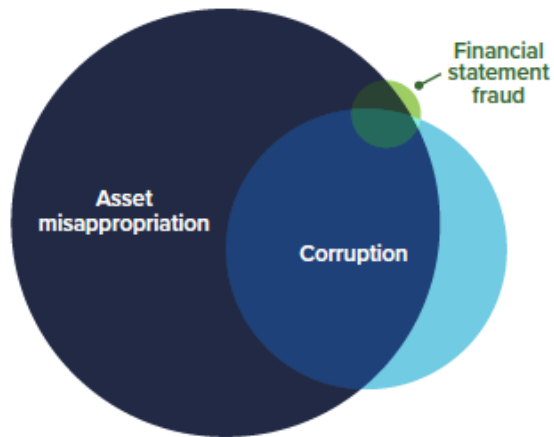
It is against this backdrop that the PwC Forensics practice embarked on its Global Economic Crime Survey, the latest in a series of studies dating back more than 20 years. In our research, conducted between January and March 2024, PwC surveyed nearly 2,500 companies across 63 territories. Two-thirds of respondents were C-suite executives—including 450 General Counsel, Chief Compliance Officers and Chief Audit Executives—and 40% were from companies with revenues greater than US\$1 billion. We also conducted over 45 interviews with senior executives from major corporations around the world to discuss their leading practices. This body of research gave us a unique lens on how today's boards and business leaders are addressing the economic crime risks their organisations are navigating daily.



What is happening?

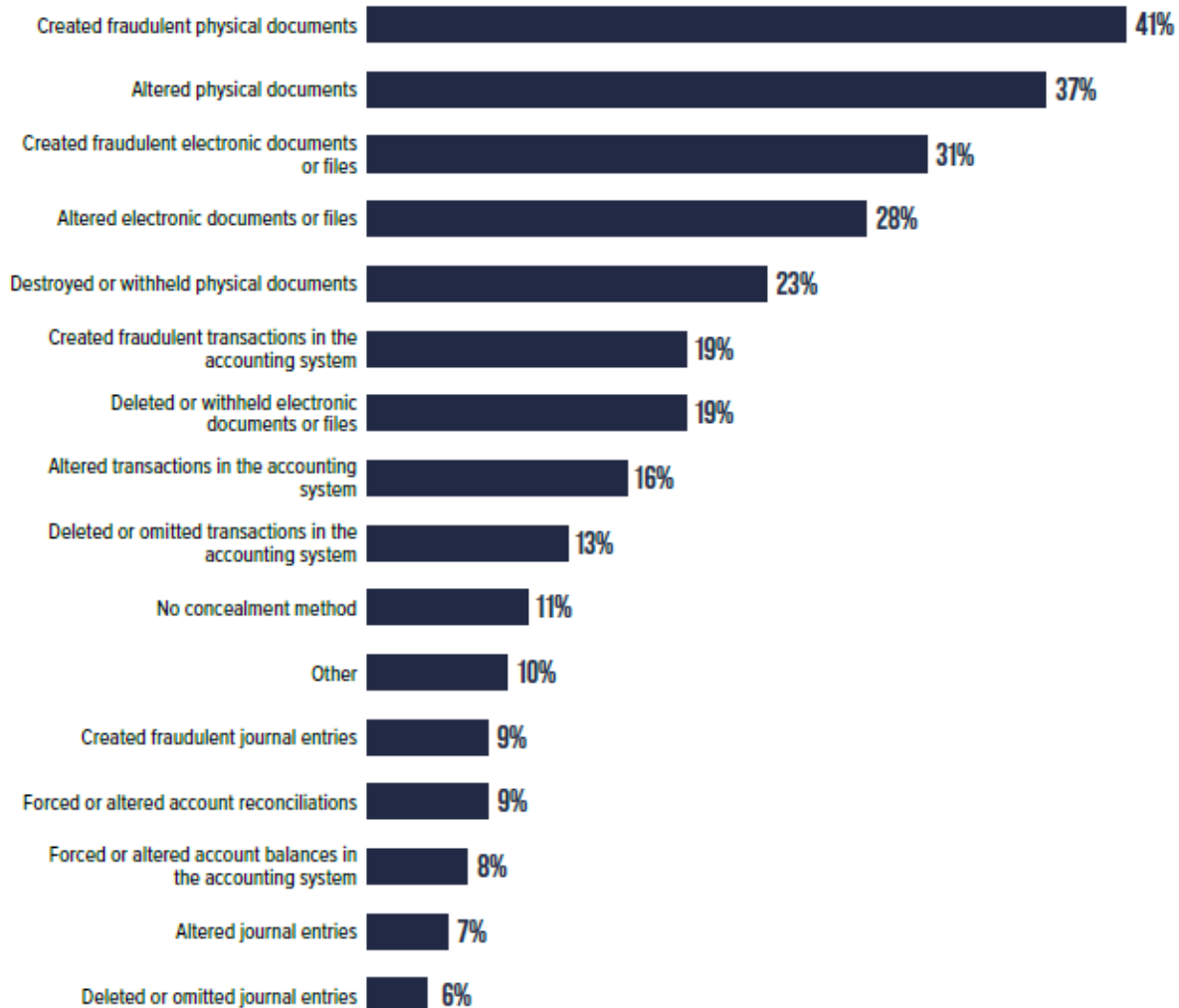


FIG. 4 HOW OFTEN DO FRAUDSTERS COMMIT MORE THAN ONE TYPE OF OCCUPATIONAL FRAUD?



Asset misappropriation only	●	51%
Asset misappropriation and corruption	●●	35%
Corruption only	●	10%
Corruption, asset misappropriation, and financial statement fraud	●●●	2%
Asset misappropriation and financial statement fraud	●●	1%
Financial statement fraud only	●	1%
Corruption and financial statement fraud	●●	<1%

FIG. 10 HOW DO OCCUPATIONAL FRAUDSTERS CONCEAL THEIR SCHEMES?



A decorative horizontal band at the top of the page features a grid of squares. Each square is divided into four quadrants, with colors including yellow, orange, pink, and grey. A large yellow circle is positioned on the left side of this band, containing the black number '3'.

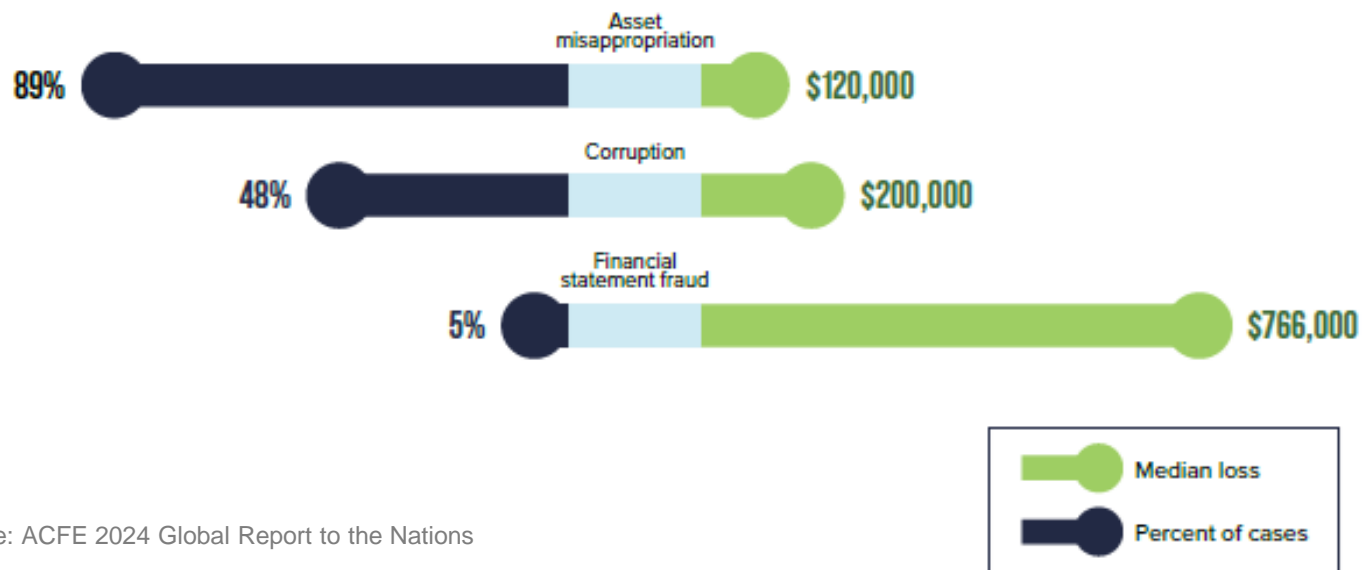
3

**Not all fraud has an equal
impact**

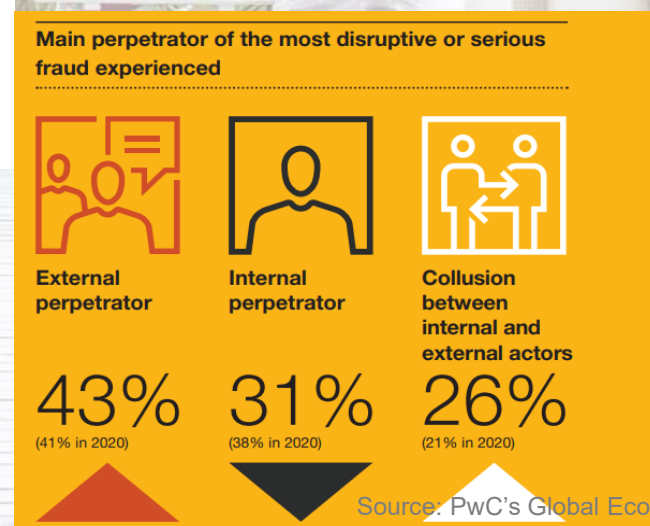
How and who?



FIG. 2 HOW IS OCCUPATIONAL FRAUD COMMITTED?



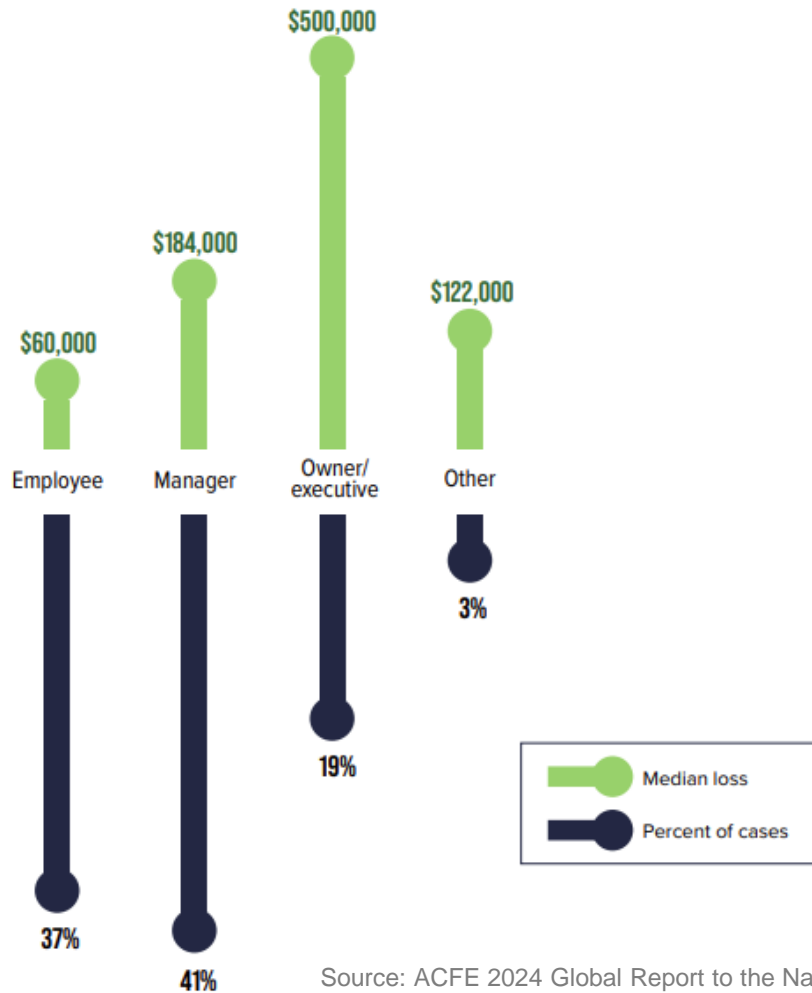
Source: ACFE 2024 Global Report to the Nations



How and who?

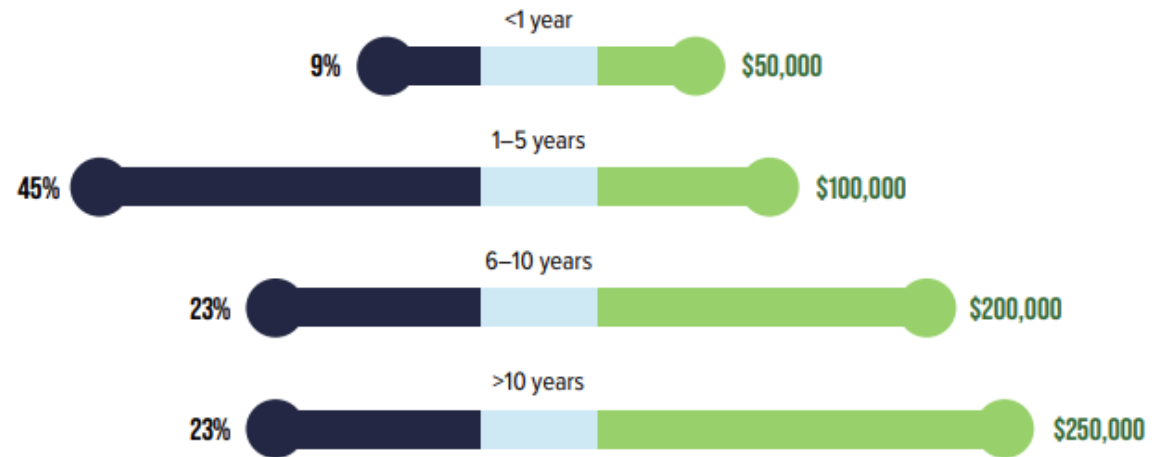


FIG. 40 HOW DOES THE PERPETRATOR'S LEVEL OF AUTHORITY RELATE TO OCCUPATIONAL FRAUD?



Source: ACFE 2024 Global Report to the Nations

FIG. 42 HOW DOES THE PERPETRATOR'S TENURE RELATE TO OCCUPATIONAL FRAUD?



How and who?



FIG. 50 HOW DOES THE NUMBER OF PERPETRATORS IN A SCHEME RELATE TO OCCUPATIONAL FRAUD?



FIG. 49 HOW DOES THE PERPETRATOR'S EDUCATION LEVEL RELATE TO OCCUPATIONAL FRAUD?

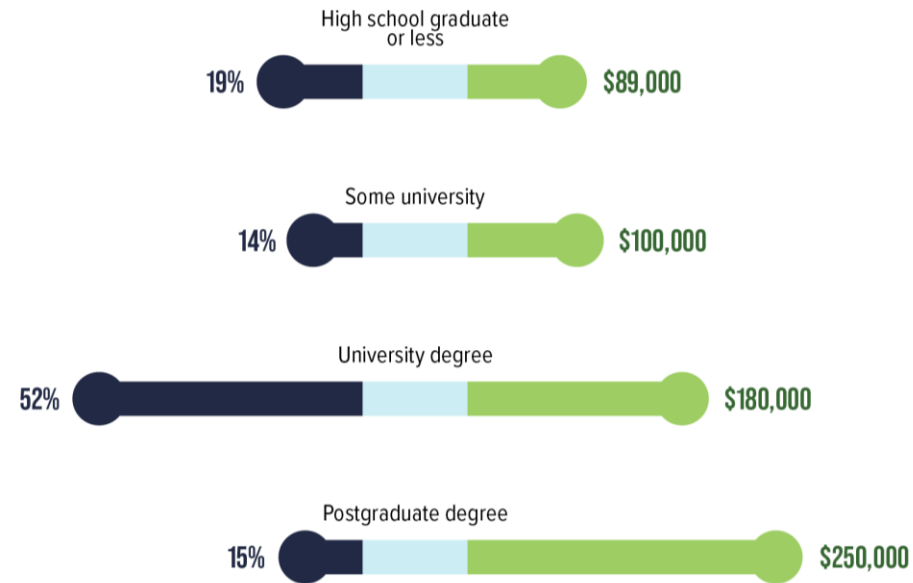
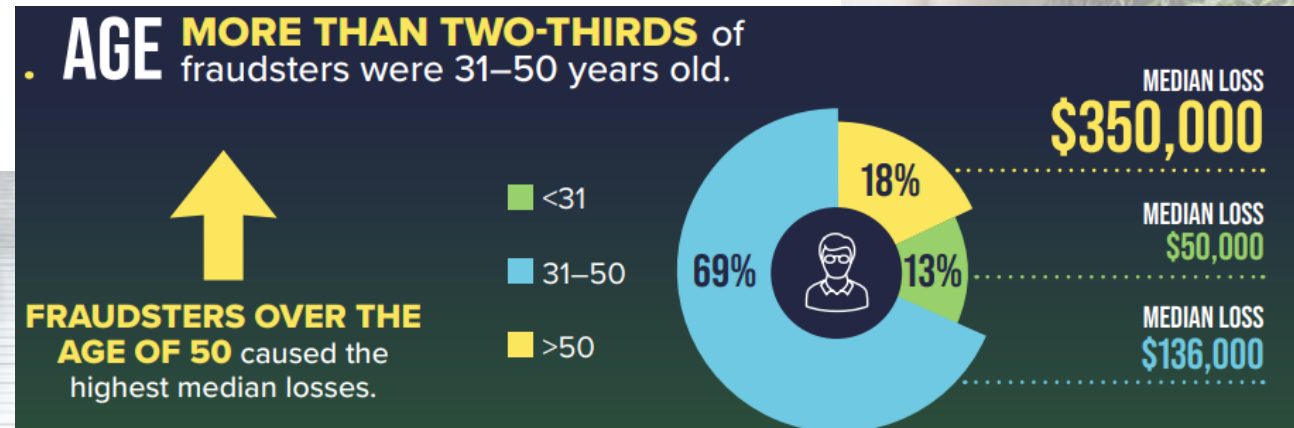
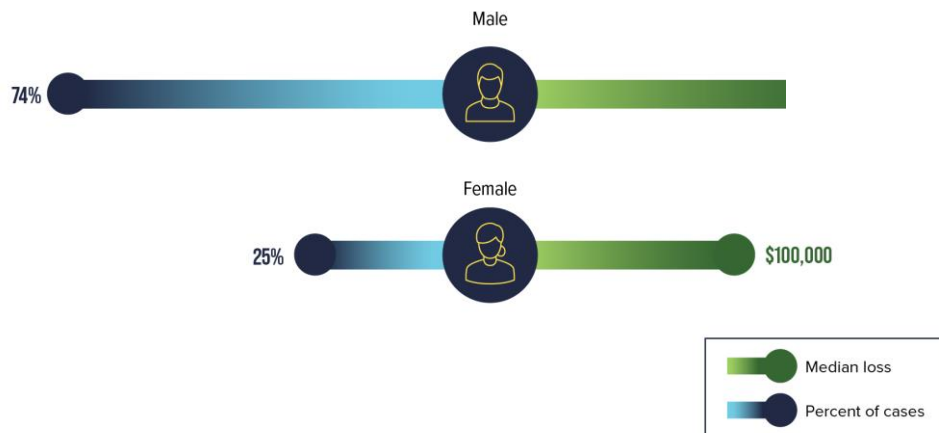


FIG. 45 HOW DOES THE PERPETRATOR'S GENDER RELATE TO OCCUPATIONAL FRAUD?



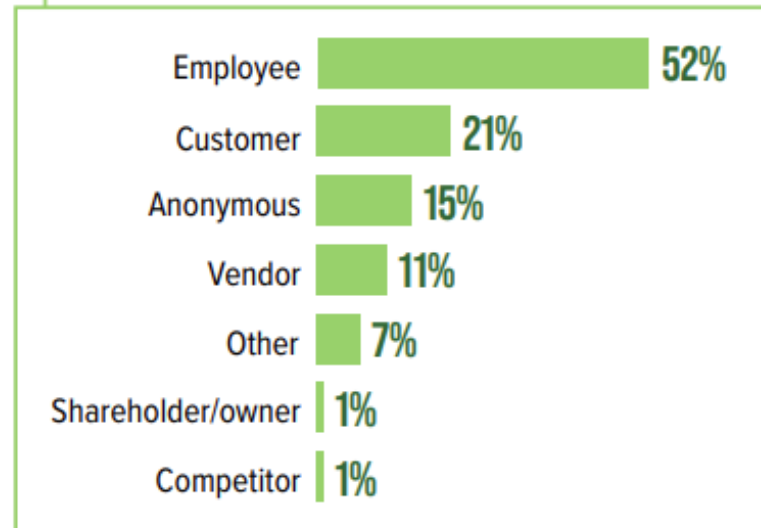
How and who?



FIG. 13 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED?



FIG. 14 WHO REPORTS OCCUPATIONAL FRAUD?



Source: ACFE 2024 Global Report to the Nations

How and who?



FIG. 17 TO WHOM DID WHISTLEBLOWERS INITIALLY REPORT?

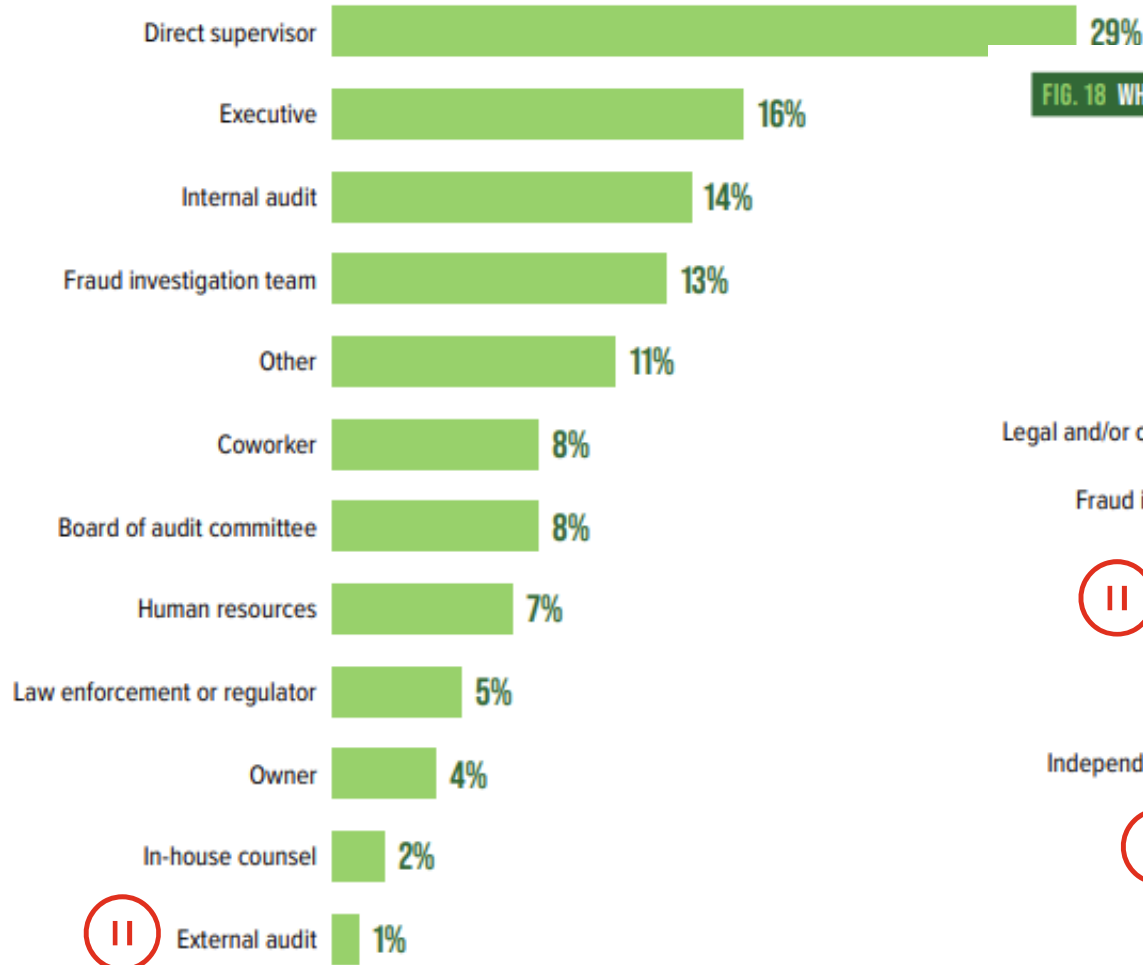
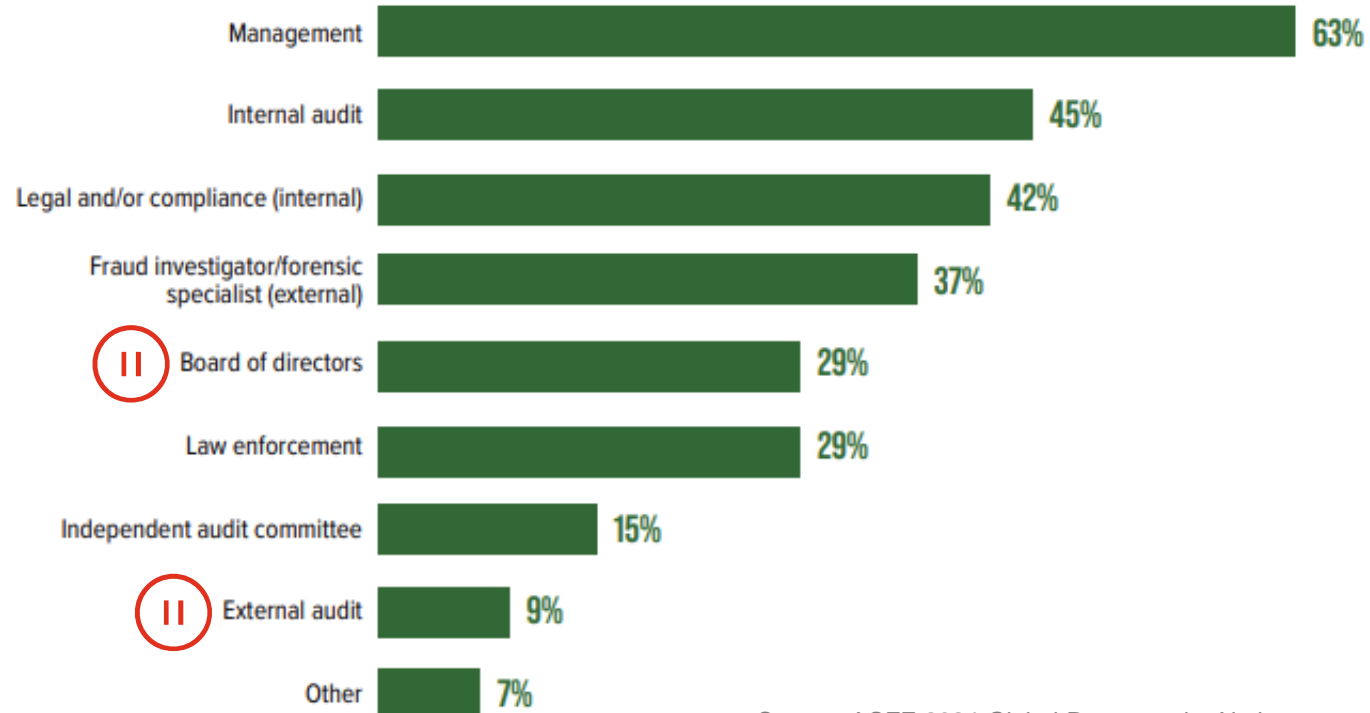


FIG. 18 WHICH PARTIES WERE ALERTED TO THE FRAUD AFTER IT WAS DISCOVERED?



Source: ACFE 2024 Global Report to the Nations



4

So what do we do about it?

Insights from leading practitioners

Our Leading Practice Interviewees had further recommendations, including:



Encourage a speak up culture.

When the company's contracts with suppliers are technically complex, the possibility of request for proposal manipulation and bid rigging is elevated. Whistleblowers are often critical to uncovering misconduct.



Explore AI and GenAI use cases.

Artificial Intelligence (AI) and Generative AI (GenAI), in combination with advanced analytics and automation, can contribute to better contract lifecycle management and assist in identifying procurement-related risks through enhanced monitoring.



Maintain a robust COI policy.

A well-defined conflict of interest (COI) policy is essential, as is regular training on that policy. Some of our interview respondents ask staff to complete both a pre-employment COI questionnaire and a post-employment certification, which together raise awareness of the risk and can increase the number of reported matters.



Strengthen defences.

Technology is unfortunately part of the problem too. Criminal organisations, some of our interviewees explained, are using AI to create fake invoices and to impersonate senior executives as part of spearfishing attacks. Other respondents emphasised the role played by employees in facilitating procurement fraud and advocated that these risks be addressed as part of the company's insider threat programme. Continuous monitoring of employee emails, where legal and feasible, was mentioned by several executives.



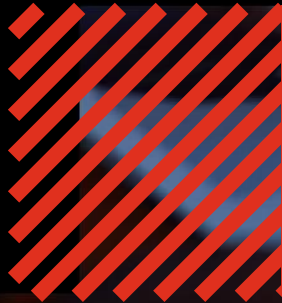
Break down silos.

Avoiding internal silos is important. The Compliance function needs to secure buy-in from procurement on a risk-based approach to third parties, including due diligence ahead of onboarding, onsite audits where appropriate and re-screening of legacy vendors. Internal Audit is another key partner, and while its risk metrics may differ from Compliance, the two functions need to team closely and have access to the other's data analytics and related dashboards.



Leverage predictive analytics.

Take steps to explore the use of AI to produce next-level predictive analytics, utilising disparate sources of data from within the company (e.g., gifts and entertainment spending, whistleblower hotline activity, human resources reviews) and about external parties (e.g., changes in use of suppliers or channel partners) that may identify business units or geographies at higher-risk.



While data to support fraud prevention and detection efforts is often plentiful and enterprise resource planning (ERP) systems reinforce good hygiene, technology isn't solely a force for good. In the hands of criminals, advanced technology also enables sophisticated efforts to perpetrate fraud.



Insights from leading practitioners

Our Leading Practice Interviewees had further recommendations, including:



Stay alert to conflicts of interest.

Companies should be alert to the fact that trade compliance violations can start with conflicts of interest, including receiving personal benefits from parties and/or individuals in sanctioned countries.



Monitor social media.

Companies that produce physical, branded products should monitor social media for images of its products being used in sanctioned countries.



Conduct crisis simulations.

Boards should encourage management to conduct crisis simulations focusing on geopolitical scenarios and, where applicable, potential for countersanctions from other countries. It is important to apply the lessons learned to the company's export controls and sanctions compliance programme and its broader business continuity plans.



Benchmark your compliance programme.

Periodically undertake compliance programme assessments designed to benchmark existing programmes against regulatory expectations and peer best practices.



Use sales data to identify diversion.


Companies need to intensify their efforts to leverage sales data to identify possible instances of diversion to sanctioned countries by third parties in neighbouring countries. Identifying specific products that are likely to be of higher value to the sanctioned countries may help focus the company's data analytics efforts.



Conduct employee surveys

Brief annual employee surveys focusing on ethics and compliance can provide useful additional data points to inform other risk management activities. Embedding these short surveys into annual compliance training can increase participation rates.

Across all of the risk areas surveyed, three common themes emerged as actions that could improve risk management and compliance: strengthening risk assessments, improving third-party risk management practices, and better leveraging data and analytics on behalf of compliance and investigations.



Where to from here

Supply chains. Markets. Competitors. Regulators. Law Enforcement.
Technological change. Complexity does not have to be your adversary.

Take risks intelligently. Develop even greater confidence in compliance.



Here are questions to ask yourself and your team—before your board or regulators ask you:

1 Is your board adequately engaged on your issues?

Sustaining strong board interest, especially after a high-profile investigation or regulatory matter has concluded, can be a challenge. Emerging issues like the need to comprehensively map your supply chain to better deal with the risk of forced labour can struggle to get time on a crowded meeting agenda. Issue-specific briefings for select directors can help. Refreshed data visualisations of key risk management data are worth exploring.

2 Does your risk appetite match that of your CEO?

With earlier and more proactive strategic engagement with your CEO, the risk function can help close the disconnect with senior leadership that can sometimes exist. See PwC's recent [Global Risk Survey](#) and [Global Internal Audit Study](#) for more information.

3 Are your risk assessments overdue for an assessment of their own?

It's time for a fresh look at geopolitical risk assumptions, new regulatory obligations and cross-border enforcement trends.

4 Will better visibility, inside and outside your company, to past incidents of employee misconduct, and your efforts to hold people accountable and mitigate the risk of future problems, help deter aberrational behaviour today?

More frequent, short surveys of employees on matters relating to ethics and compliance can provide useful data points for the second and third lines of defence. Benchmarking your communications strategy against the leaders, including firms outside your industry, is a worthwhile exercise.

5 Are the investigation capabilities at your disposal going to establish the facts as quickly as you need them?

Upskilling the data analytics and AI capabilities of your team, including the tools they utilise, is a sound investment. Critical decisions—whether about the veracity of a whistleblower or the benefits of self-reporting—are informed by the quality of the data analysis.

6 Are you measuring fraud losses adequately and getting to root causes?

Perhaps a wider perspective is required to be more confident that similar risks aren't lurking in other parts of the business.

7 Is your third-party risk management approach up to the challenge?

You may have access to the data you need today, but the data *you want* is a different story. Stronger teaming between Compliance, Internal Audit and Procurement could secure the data lake and analytics capabilities you need to unlock compliance insights.



Thank you

© PwC. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.

Fraud Landscape 2: Fraud Risk Management Frameworks and Tools presented by Manuel Caldeira



Position: Associate Partner in EY's Forensics & Integrity Services division in Sandton.

Qualifications: CA(SA), Certified Fraud Examiner (CFE), and Certified Anti-Money Laundering Specialist (CAMS).

Experience: Over 25 years of experience in audit and consulting, dedicated the last 12 years to forensic services, honing his expertise in financial crime and fraud risk management.

Mission-Driven: Manuel is driven by EY's mission to build a better working world. He strives to create an environment free from the devastating effects caused by financial crime, not only for EY's clients but also for all future generations in Africa.



Fraud Risk Management Frameworks and Tools

The IRBA Indaba

6 August 2024

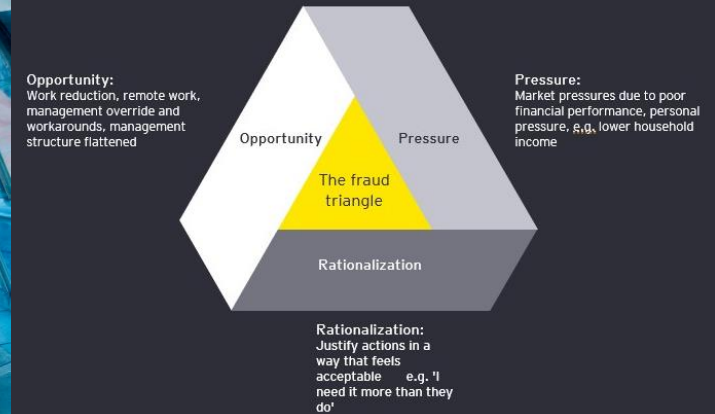


EY

Building a better
working world

Learning objectives

1. **Why** is Fraud Risk Management important?
2. **What** fraud guidance is available from IRBA
- How** to evaluate Fraud Risk Management Maturity:
 3. Association of Certified Fraud Examiners: Fraud Resources
 4. The COSO Fraud Risk Management Guide
 5. ACFE Fraud Risk Management Scorecards



Willingness to act without integrity appears to be on the rise.

Nearly four out of 10 (**38%**) global respondents admit they'd be **prepared to behave unethically in one or more ways to improve their own career progression or remuneration – more than one and a half times higher than the findings in our last report.**

1. Why is Fraud Risk Management important

• Once upon a time...

- An audit client was losing millions per month due to fraud related losses
- Management could not understand this as they had put in very expensive fraud tools to prevent and detect the fraud events and had many people running around responding to the detected Fraud events
- The auditors wanted to better understand managements capability of preventing and detecting fraud so as part of their response to Fraud Risk carried out a Fraud Risk Management Maturity Assessment with the support of their Forensics team. This identified several FRM process gaps to international best practices including lack of regular Fraud Risk Assessments by some of the business units where fraud losses were increasing
- The management of the business units disputed these findings, but auditors shared these findings with those charged with governance who by now had serious concerns related to the increasing significant fraud events
- At year end, fraud losses increased considerably and the audit committee instead of questioning the auditors why they had not picked this up, asked management why they had not taken the audit recommendations seriously
- Management addressed the findings raised by the audit team in the following year and with improved Fraud Risk Management in place, fraud losses began to drop due to the regular Fraud Risk Assessment helping the client identify emerging fraud risks and then updated fraud controls to prevent and detect these in a timely manner



2. IRBA Fraud Guidance – a closer look at What guidance is available

The screenshot shows the IRBA website header with navigation links: EVENTS, FRAUD PREVENTION, TIP-OFF, WHISTLEBLOWING: CALL 0800 212 208, MANUAL OF INFORMATION, IFAC, Login, and a search icon. Below the header is a navigation menu: Home, About Us, Guidance for RAs, Library, Become an RA, Find an RA, Registry, News & Events. The main banner features a pink lotus flower and the word 'Integrity' in large white text. Below the banner is a breadcrumb trail: Home » Guidance for RAs » Technical Guidance for RAs » Staff Practice Alerts » Fraud. A sidebar on the left contains 'IFRS 9 and ISA 720' and 'Fraud'. The main content area is titled 'Fraud Guidance' and contains a paragraph: 'Below is a list of links to relevant guidance on Fraud, which have been developed internationally and locally. The list references information that was known at the time of issuing this [IRBA Staff Audit Practice Alert: A South African Perspective on the Auditor's Considerations Relating to Fraud](#) and it is not meant to be exhaustive.' A list of links follows, with the first link highlighted in yellow: '> [SAICA Frequently Asked Questions: Application of the requirements of the International Standards on Auditing in relation to matters arising from monitoring findings and other in-practice challenges – The presumption of risks of fraud in revenue recognition \(page 4\)](#)'. A red arrow points from a text box on the right to this highlighted link.

IRBA STAFF AUDIT PRACTICE ALERT 4: A SOUTH AFRICAN PERSPECTIVE ON THE AUDITOR'S CONSIDERATIONS RELATING TO FRAUD

IMPLEMENTATION GUIDANCE TO RESPOND TO THE RISKS OF MATERIAL MISSTATEMENTS DUE TO FRAUD

1. The implementation guidance contained in this IRBA Staff Audit Practice Alert includes the following key themes:

- The primary responsibility for the prevention and detection of fraud rests with those charged with governance of the entity and management;

Home » Guidance for RAs » Technical Guidance for RAs » Staff Practice Alerts » Fraud

IFRS 9 and ISA 720 >

Fraud

Fraud Guidance

Below is a list of links to relevant guidance on Fraud, which have been developed internationally and locally. The list references information that was known at the time of issuing this [IRBA Staff Audit Practice Alert: A South African Perspective on the Auditor's Considerations Relating to Fraud](#) and it is not meant to be exhaustive.

- > [SAICA Frequently Asked Questions: Application of the requirements of the International Standards on Auditing in relation to matters arising from monitoring findings and other in-practice challenges – The presumption of risks of fraud in revenue recognition \(page 4\)](#)
- > [Transparency International: Corruption Perceptions Index](#)
- > [Association of Certified Fraud Examiners: Fraud Resources](#)
- > [Institute of Commercial Forensic Practitioners: Industry Research](#)
- > [AICPA Frequently Asked Questions: Audit Matters and Auditor Reporting Issues Related to COVID-19 – Fraud Inquiries \(page 12\)](#)
- > [Center for Audit Quality: Managing Fraud Risk, Culture, and Skepticism During COVID-19](#)

Are those charged with governance and management capable of preventing and detecting fraud?

Do auditors know which questions to ask?

Is there an international framework that auditors can use?

[Link: Fraud Guidance - IRBA](#)

3. Association of Certified Fraud Examiners: Fraud Resources (How)

ACFE
Association of Certified Fraud Examiners

Together, Reducing Fraud Worldwide

About the ACFE

Membership ▾ CFE Credential ▾ Fraud Resources Library ▾ Community ▾ Training, Events and Products ▾

Home

Fraud Resources

Curated and created for anti-fraud professionals, find the latest news, trends, analysis, topics and reports in these ACFE resources

Share: [in](#) [f](#) [x](#) [e](#)

Featured Resources | Report to the Nations | Topics & Resource Types | Publications | Tools

Featured Resources

Occupational Fraud 2024: A Report to the Nations →

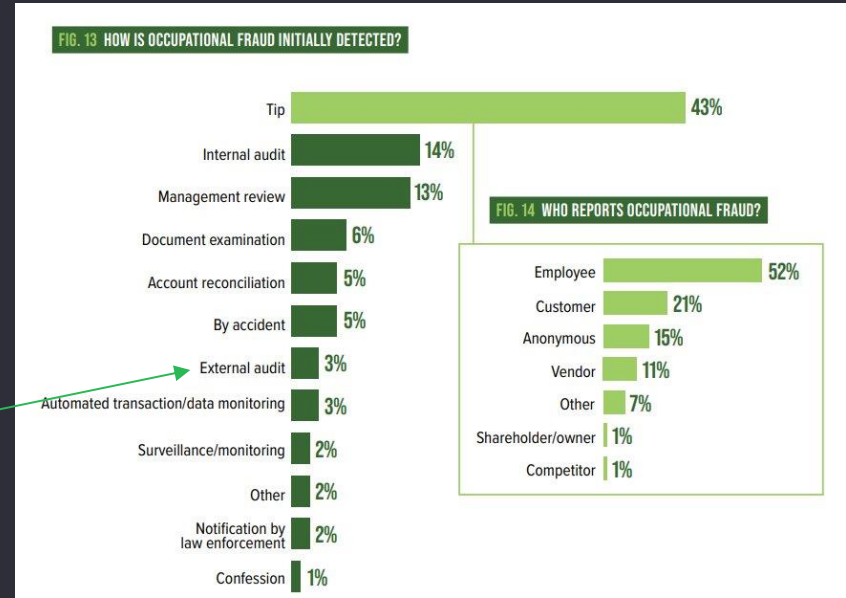
The 13th edition of the world's largest study on occupational fraud analyzes 1,921 actual cases, providing updated guidance and new findings from fraud schemes that likely occurred at the height of the COVID-19 pandemic.

2024 Anti-Fraud Technology Benchmarking Report →

Developed in partnership with SAS, this report explores emerging trends and aids in assessing the effectiveness of anti-fraud technology toolkits and planning for future technology-related budgets and resources.

The Fraud Risk Management Guide →

To provide best-practices guidance for assessing and managing fraud risks, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) partnered with the Association of Certified Fraud Examiners (ACFE) to create the Fraud Risk Management Guide.



BENCHMARK YOUR ORGANIZATION

Compare your organization's fraud risks by industry, region and size. Benchmark your anti-fraud efforts against similar organizations and against the most effective methods for reducing fraud losses.

MORE THAN HALF OF OCCUPATIONAL FRAUDS OCCUR DUE TO LACK OF INTERNAL CONTROLS OR AN OVERRIDE OF EXISTING INTERNAL CONTROLS.

- LACK OF INTERNAL CONTROLS (32%)
- OVERRIDE OF EXISTING CONTROLS (19%)

[Link: Fraud Resources \(acfe.com\)](https://www.acfe.com)

Source: 2024 ACFE Report to the Nations

4. The COSO Fraud Risk Management Guide

FRAUD RISK MANAGEMENT GUIDE Second Edition

Guide Tools Resources Home

The Fraud Risk Management Guide

To provide **best-practices guidance for assessing and managing fraud risks**, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) partnered with the Association of Certified Fraud Examiners (ACFE) to create the Fraud Risk Management Guide. The report is designed to aid organizations in effectively establishing a comprehensive fraud risk management program. It specifically identifies how they can:

- Establish fraud risk governance policies
- Perform fraud risk assessments
- Design and deploy fraud prevention and detection control activities
- Conduct fraud investigations
- Monitor and evaluate the effectiveness of the fraud risk management program

Purchase the Fraud Risk Management →

FRAUD RISK MANAGEMENT GUIDE Second Edition

COSO Association of Certified Fraud Examiners ACFE

COSO revised its *Internal Control — Integrated Framework* in 2013 to incorporate 17 principles. These 17 principles are associated with the five internal control components COSO established in 1992. The principles provide clarity for the user in designing and implementing systems of internal control and for understanding requirements for effective internal control. COSO clarifies that for a system of internal control to be effective, each of the 17 principles is present, functioning, and operating in an integrated manner. Throughout this Guide the COSO 2013 IC Framework has been used as a source for describing aspects of internal control.

Principle 8, one of the risk assessment component principles, states:
The organization considers the potential for fraud in assessing risks to the achievement of objectives.

This Guide is intended to be supportive of and consistent with the COSO 2013 IC Framework and can serve as guidance for organizations to follow in performing a fraud risk assessment.

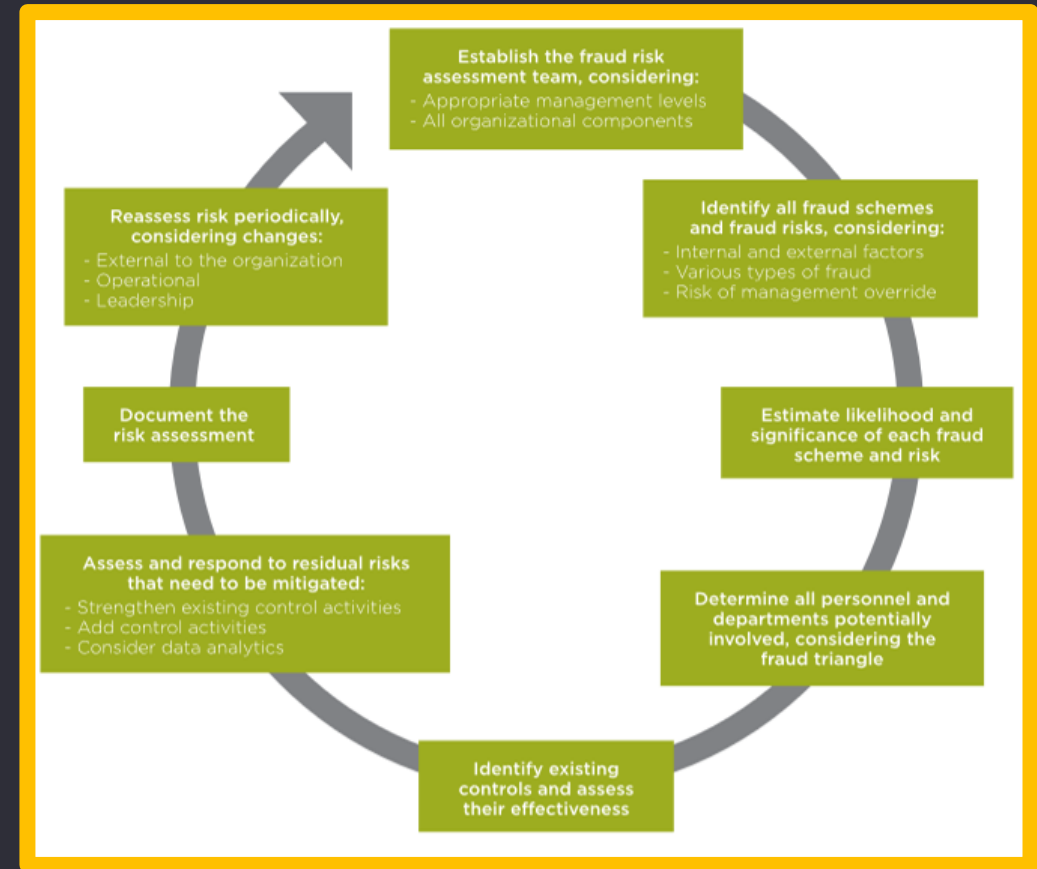
Free Executive Summary

The Executive Summary provides a high-level overview of the guide and is intended for boards of directors and senior management. It explains the benefits of establishing strong anti-fraud policies and controls.

Download the Executive Summary →

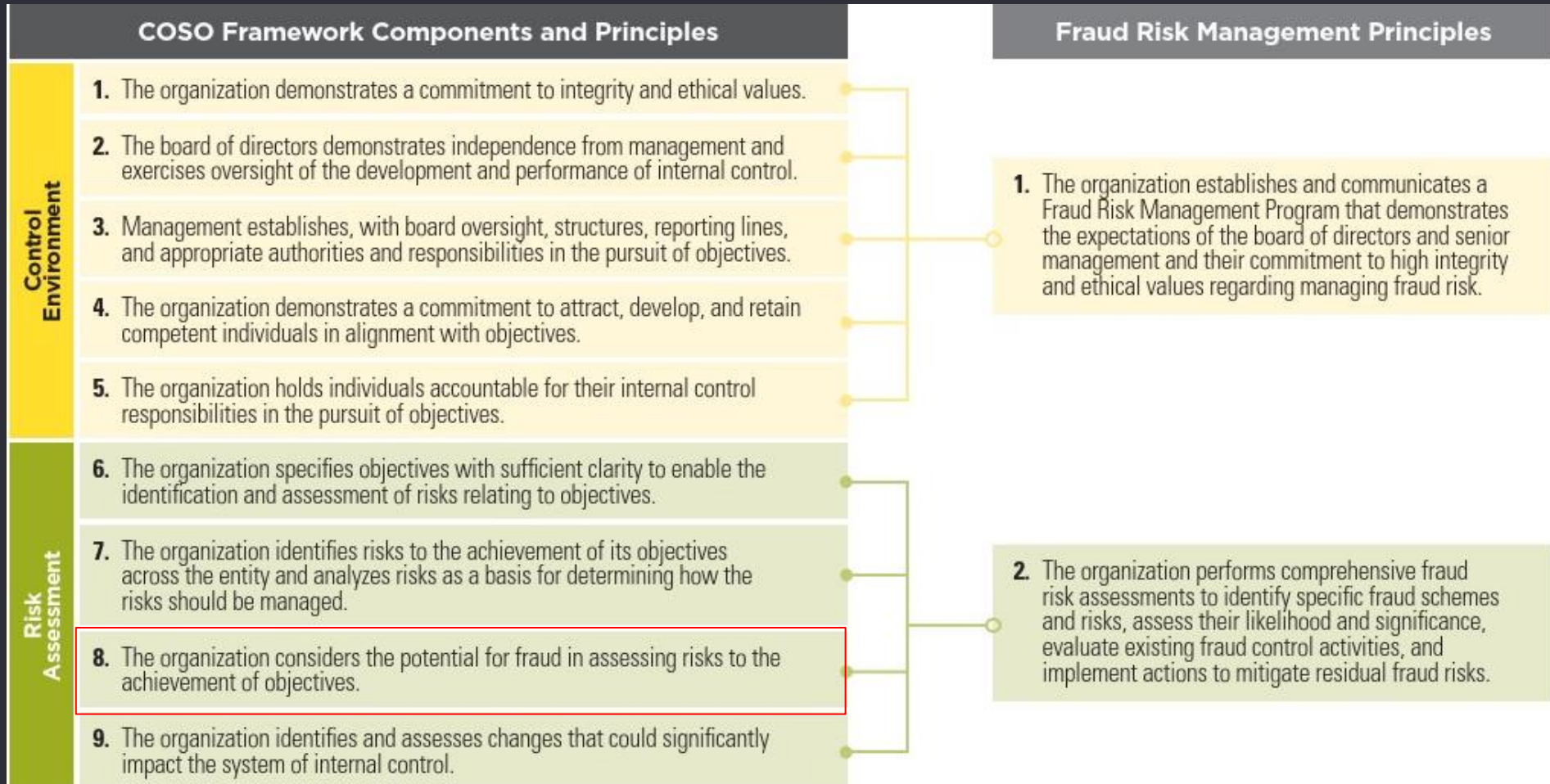
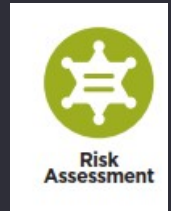
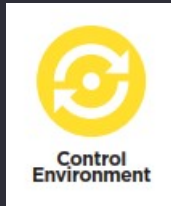
Source link: <https://www.acfe.com/fraud-resources/fraud-risk-tools---coso/fraud-risk-management-guide/>

4.1. The COSO Fraud Risk Management Guide – Fraud Risk Assessment overview



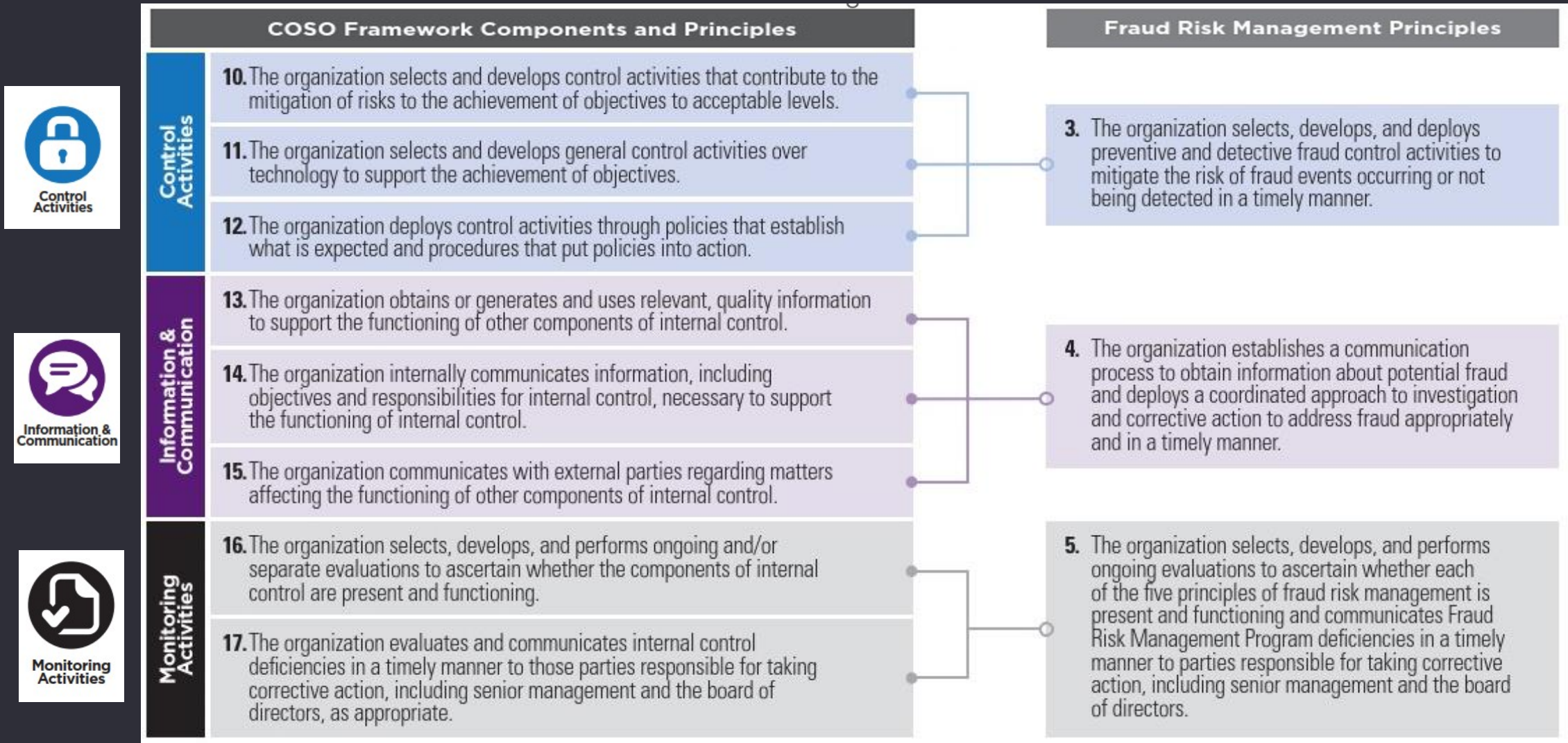
Source: [coso-fraud-risk-management-guide-second-edition-executive-summary.pdf \(acfe.com\)](https://www.acfe.com/coso-fraud-risk-management-guide-second-edition-executive-summary.pdf)

4.2. COSO Fraud Risk Management Guide – 5 Principles of FRM




Source: [coso-fraud-risk-management-guide-second-edition-executive-summary.pdf \(acfe.com\)](https://www.acfe.com/coso-fraud-risk-management-guide-second-edition-executive-summary.pdf)

4.2. COSO Fraud Risk Management Guide – 5 Principles of FRM (continued)



Source: [coso-fraud-risk-management-guide-second-edition-executive-summary.pdf \(acfe.com\)](https://www.acfe.com/coso-fraud-risk-management-guide-second-edition-executive-summary.pdf)

5. ACFE Fraud Risk Management Scorecards



FRAUD RISK MANAGEMENT GUIDE Second Edition

ACFE Association of Certified Fraud Examiners

[GUIDE](#) [TOOLS](#) [RESOURCES](#)

Fraud Risk Management Scorecards

The fraud risk management scorecards can be used to assess each of the five fraud risk management principles to aid in determining how comprehensive an organization's fraud risk management program is and how well it is achieving its objectives. (For more information about each of the five fraud risk management principles, see the *COSO Fraud Risk Management Guide*).

Please select a fraud risk management principle in the drop-down menu and then click the button below to begin an assessment.

NOTE: Your scorecard input and results will not be saved once you leave this site, so you will need to download or print your results at the end of each assessment. To begin a new session on a scorecard you have previously completed, please close and reopen your browser.

Select a fraud risk management principle:

Principle 1: Fraud Risk Governance

Begin Assessment

Source: [Fraud Risk Tools \(acfe.com\)](https://www.acfe.com)

Fraud Risk Governance Scorecard

[Download Report \(PDF\)](#) [Download Report \(CSV\)](#)

Summary by Points of Focus

Point of Focus	Score
MAKING AN ORGANIZATIONAL COMMITMENT TO A FRAUD RISK MANAGEMENT PROGRAM	
SUPPORTING FRAUD RISK GOVERNANCE	
ESTABLISHING A COMPREHENSIVE FRAUD RISK MANAGEMENT POLICY	
ESTABLISHING FRAUD RISK GOVERNANCE ROLES AND RESPONSIBILITIES THROUGHOUT THE ORGANIZATION	
DOCUMENTING THE FRAUD RISK MANAGEMENT PROGRAM	
COMMUNICATING FRAUD RISK MANAGEMENT AT ALL LEVELS OF THE ORGANIZATION	
USING DATA ANALYTICS TO SUPPORT FRAUD RISK GOVERNANCE	

Fraud Risk Governance Scorecard (Fraud Risk Governance)

To assess the strength of the organization's fraud governance, carefully assess each area below and score the area, factor, or consideration as:

- Red: indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk
- Yellow: indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down
- Green: indicating that the area, factor, or consideration is strong and fraud risk has been reduced — at least — to a minimally

Each area, factor, or consideration scored either red or yellow should have a note associated with it that describes the action plan for bringing it to green on the next scorecard.

Fraud Risk Governance Area, Factor, or Consideration	Score	Notes
MAKING AN ORGANIZATIONAL COMMITMENT TO A FRAUD RISK MANAGEMENT PROGRAM		
Our organization has a strong correlation between our organizational culture and fraud risk management.	●	No evidence
Our organization's leadership demonstrates "tone at the top" by promoting ethical behavior and emphasizing a focus on deterring, preventing and detecting fraud.	●	CEO Speech contained...
Our organization's leadership leads by example to ensure that all personnel, vendors, and contractors understand that the organization is serious about promoting ethical behavior and is committed to deterring, preventing and detecting fraud.	●	Strong ethical behavior

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

© 2024 EYGM Limited.
All Rights Reserved.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

Thank You



Fraud Landscape 3: Cybersecurity, Financial Reporting and Audit presented by Lucien Pierce



Position: Director at PPM Attorneys

Advisory Role: Lucien advises both state and private clients on information security matters, including compliance with data protection regulations and appropriate responses to data breaches.

Specialised Expertise:

- Information Technology Outsourcing and E-commerce
- Telecommunications and Broadcasting Regulatory Law
- Intellectual Property Issues
- Corporate Governance

Legal Knowledge: Lucien is well-versed in the legal aspects of information security, particularly data protection and privacy.

PPM

ATTORNEYS

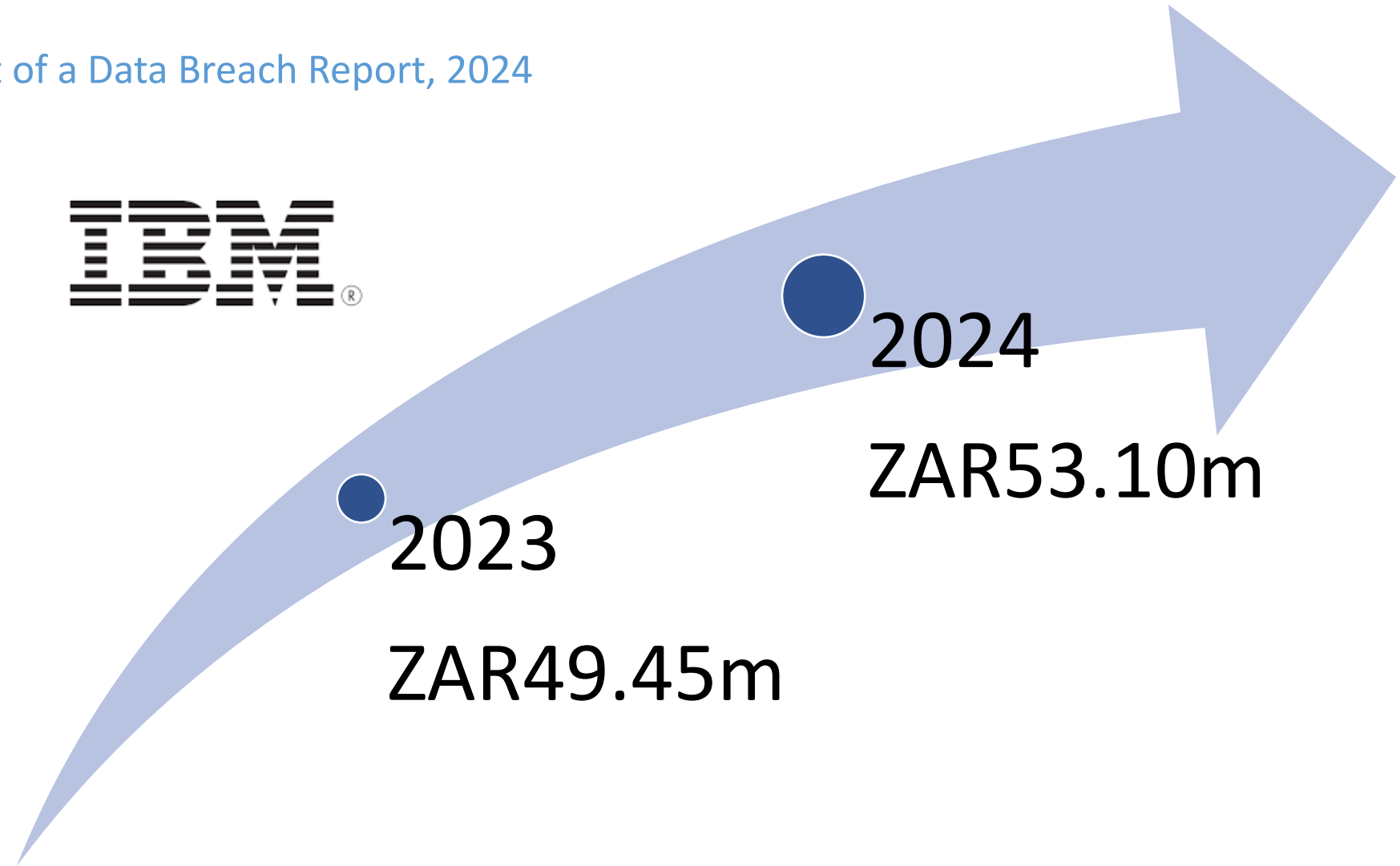
Cybersecurity, Financial Reporting and Audit
The IRBA Indaba, 6th August 2024



Why report cyber-risks in financials?

Cost of a Data Breach Report, 2024

IBM[®]



What are cyber-risks?



Data breach



Ransomware



Critical infrastructure



Business email compromise



Emerging technology risks

Why does it matter to auditors?

ISA 250(Revised)(6)(b)

Consideration of Laws and Regulations in an Audit of Financial Statements

“Other laws and regulations that do not have a direct effect on the determination of the amounts and disclosures in the financial statements, but compliance with which may be fundamental to the operating aspects of the business, to an entity’s ability to continue its business, or to avoid material penalties...non-compliance with such laws and regulations may therefore have a material effect on the financial statements...”

Cyber-related laws & regulations

-  Prudential Authority (SARB) – Directive on Cloud Computing and Offshoring of Data
-  Joint Standard 2 of 2024 – Cybersecurity and cyber-resilience
-  The Banks Act, 1990
-  The Financial Sector Regulation Act, 2017
-  Protection of Personal Information Act, 2013
-  Critical Infrastructure Protection Act, 2019
-  Cybercrimes Act, 2020
-  National Cloud & Data Policy, 2024
-  Next Generation Radio Frequency Spectrum Policy, 2024



Case studies on cyber-related risks

ENS and PSG;

SA Post Office

Department of Public Works

SolarWinds;

CrowdStrike; and

Emerging technologies like artificial intelligence



Thank you!

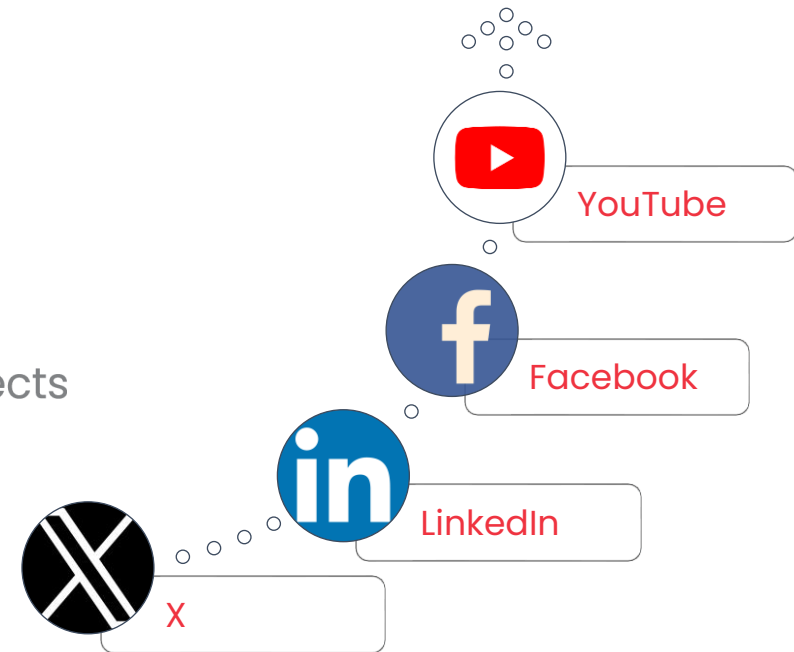
- Any questions?
- Follow us on our social media pages to learn more about cybersecurity, data privacy and technology law developments in South Africa

PPM

A T T O R N E Y S

Information Security | Media | Technology | Infrastructure Projects

www.ppmattorneys.co.za



Q&A Part 1





Tea / Comfort Break

We will recommence at 14:45

