ORIGINAL
THINKING

A GUIDE TO CONDUCTING AN INTERNAL **CORPORATE INVESTIGATION**

TABLE OF CONTENTS

THE TERMS “FRAUD”, “BRIBERY”, AND “CORRUPTION” HAVE SADLY BECOME ALL TOO FAMILIAR FOR MANY SOUTH AFRICANS. IT’S HARD TO GO A DAY WITHOUT HEARING OF YET ANOTHER FRAUDULENT OR CORRUPT SCHEME.

INTRODUCTION

Since the release of the findings from the Commission of Inquiry into State Capture (colloquially known as the Zondo Commission) and South Africa’s recent “grey-listing” by the Financial Action Task Force (“FATF”), scouring fraud and corruption-related media reports has become something of a national pastime.

However, these problems are not confined to South Africa or any particular industry or sector. They are, in fact, global concerns. International regulators are becoming more visible and taking an active role in combatting fraud, bribery and corruption. In 2021, Goldman Sachs Group Inc. topped the list of the largest sanctions ever under the Foreign Corrupt Practices Act (FCPA), following a $USD.3-billion settlement with the U.S. Department of Justice and Securities and Exchange Commission. Former senior employees accused Goldman Sachs of paying more than USD1.6-billion in bribes to third-party intermediaries and high-ranking government officials in Malaysia and the UAE.

Regulators such as the U.S. Department of Justice, Securities and Exchange Commission, the U.K. Serious Fraud Office and the French National Financial Prosecutor’s Office are imposing significant sanctions on persons and companies found guilty of fraud, bribery and corruption. These international regulators are also collaborating with each other more closely than ever before. For instance, collaborative efforts of the US, UK and French regulators culminated in the USD4-billion corruption settlement with Airbus.

Importantly, the ripple effects of fraud, bribery, and corruption are not restricted to large corporations or multinational enterprises. Small businesses, too, can become embroiled in these issues, suffering potentially devastating consequences.

This guide aims to provide a comprehensive overview of how to conduct internal corporate investigations, helping you safeguard your company—regardless of its size—against the risks and repercussions of unethical conduct.

1 PART ONE

INTERNAL INVESTIGATIONS 101

WHAT IS AN INTERNAL INVESTIGATION?

An internal investigation refers to the process adopted by a company or entity to probe and uncover potential misconduct committed by management, employees, or third parties. The following are some examples of events that may necessitate an internal investigation:

- Stock theft / IP theft
- Conflicts of interest / misuse of company assets
- Procurement fraud / payment of bribes or kickbacks
- Employee misconduct, including sexual harassment, bullying, nepotism, etc
- Fraud / embezzlement
- A data breach

Essentially, an internal investigation is an inquiry into allegations of misconduct, unethical behaviour, policy violations, fraud, or any other matter that may pose a risk to the organization's integrity or reputation. Typically, internal investigations are carried out by a designated team within the organisation but often, independent, external persons may be involved.

WHEN IS AN INTERNAL INVESTIGATION TRIGGERED?

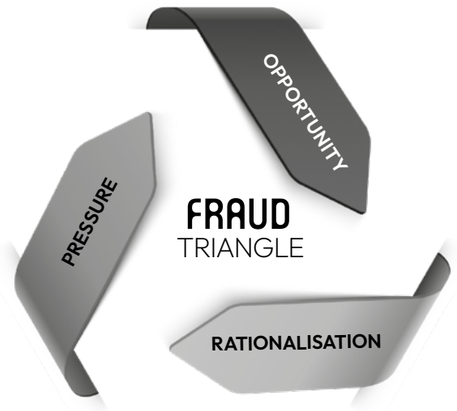
An internal investigation is often triggered by a specific event, such as:

- The belief that company data has been stolen by a current or former employee. This is more common than one may realise because intellectual property is a desirable and valuable commodity. It could take the form of a client list, a contract template, or the formulae to your most popular (and lucrative) product. There are many red flags to look out for, including:
  - An employee's abrupt departure from the company,
  - A former employee's new employment with a competitor, or
  - A data leak or unauthorised access to company records.
- Receipt of a tip-off / whistle-blower allegation. Whistle-blowing plays a vital role in encouraging accountability, transparency, and good governance. However, it's important to navigate potential challenges associated with whistle-blowers, ensuring disclosures are made in good faith and not for personal gain. In South Africa, whistle-blowers are protected by the Protected Disclosures Act 26 of 2000 (the "**Protected Disclosures Act**"), which aims to encourage whistle-blowing in the workplace and makes it easier to disclose information about criminal and other irregular conduct. Although whistle-blower complaints can be a valuable source of information, companies need to be mindful of the potential challenges when dealing with such complaints.
- External data breaches. Data breaches are becoming more and more common in today's digital environment. An internal investigation may be needed to investigate the source of the breach and identify control weaknesses.
- Being the subject of adverse media. When adverse information is published about a company in the media, irrespective of whether there is any merit to the published article or allegations, a company must be seen to take complaints and allegations seriously. As with managing a whistle-blower complaint, it is good practise to launch an internal investigation to help the company understand whether there is any truth to the allegations and how best to manage the situation.
- Increased regulatory scrutiny within the industry or jurisdiction in which a company operates. Regulators often conduct periodic reviews of different industries. As a result, companies that operate within those industries or jurisdictions come under increased scrutiny. Changes in legislation may also bring about heightened regulatory scrutiny. Companies may be required to investigate to ensure they are operating in compliance with updated legislative frameworks.
- Red flags or malfeasance identified through audit checks. Often auditors or routine checks may reveal red flags or possible malfeasance which may warrant a more comprehensive internal investigation.

WHY DO YOU NEED TO CONDUCT AN INTERNAL INVESTIGATION?

Internal investigations serve numerous purposes, including mitigating and recovering financial losses, safeguarding a company's credibility and reputation, and maintaining consumer trust and investor relations.

Internal investigations also play a significant role in minimising ongoing risks. Allowing a culture of overlooking misconduct creates opportunities, justifications, and motivation for others within the company to engage in fraud or violate company policies. By conducting an investigation into alleged wrongdoing, you reduce the risk associated with two of the three pillars of the Fraud Triangle, a framework commonly used to explain why individuals choose to commit fraud. Namely, opportunity and rationalisation.



WHO NEEDS TO BE INVOLVED IN AN INTERNAL INVESTIGATION?

In the past, it was commonly believed that internal investigations were the sole responsibility of "compliance" or "internal audit" functions. However, the reality is that leadership, middle management, human resources, finance, procurement, IT, legal, compliance and internal audit functions all have a part to play.

Whilst it is true that the investigation may be driven by a compliance or corporate investigation function (and they will be the ones doing the 'heavy lifting'), an effective investigation requires buy-in at all levels and more often than not, across departments.

The involvement of external stakeholders such as lawyers, auditors or even regulators themselves may also be necessary. Additionally, the nature or complexity of the investigation may require the expertise of subject matter experts such as:

- Legal experts for advising on legal obligations,
- Data privacy experts for handling data across different jurisdictions,
- Digital forensic and eDiscovery experts for evidence analysis and data analytics and
- Chartered accountant experts for financial statement analysis.

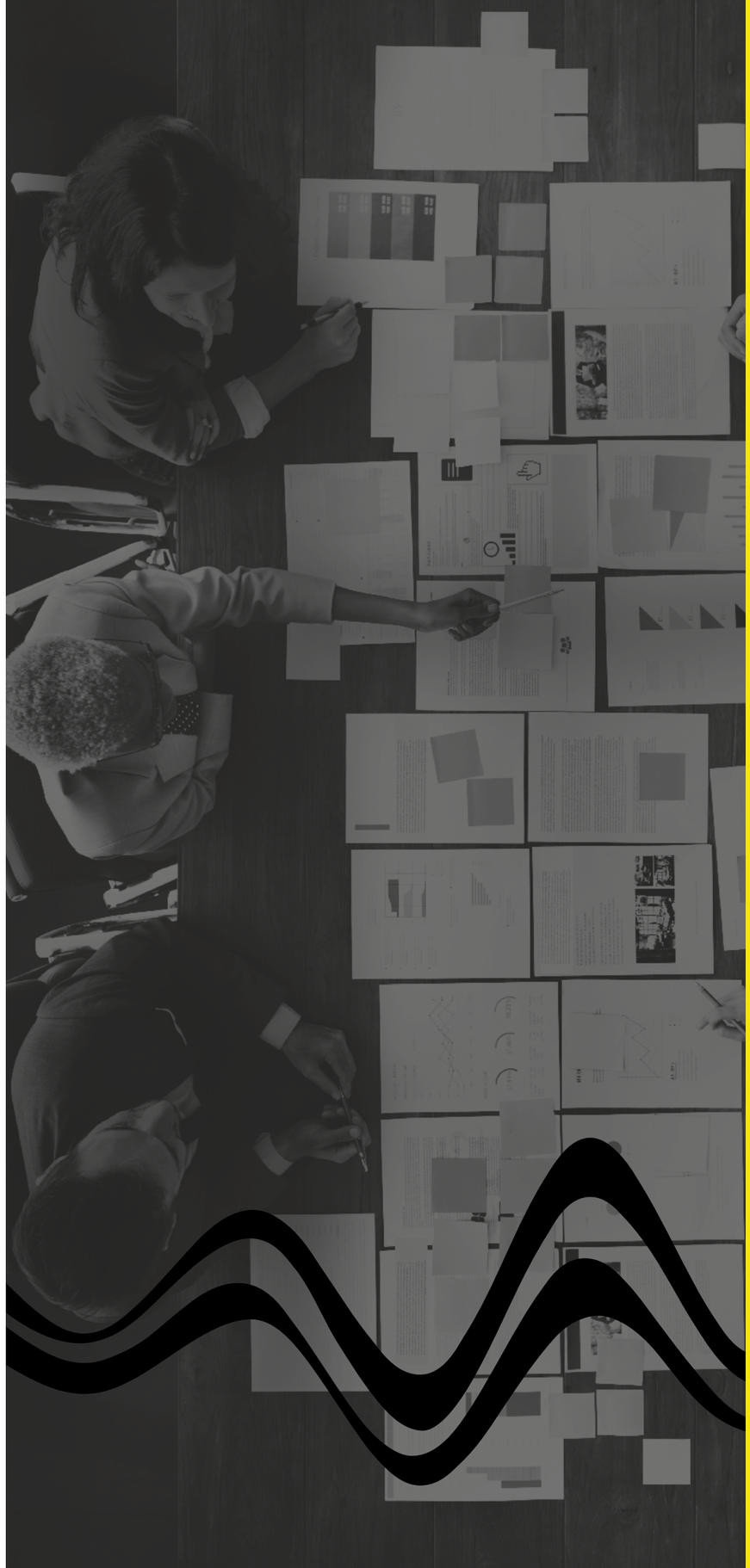
Effective stakeholder management is crucial for achieving meaningful outcomes in an investigation.

WHERE TO BEGIN?

The initial planning of any investigation is a critical step to its success. Proper planning ensures alignment with internal and external stakeholders, and raises awareness of the investigation's potential impact on the business. The investigation plan should set out the investigation's scope and establish anticipated timelines for key milestones, such as data preservation, interviews, and interim reporting. It should also consider any business deadlines that may influence the investigation's time sensitivity, such as year-end financial reporting or contractual periods.

The investigation plan should also set out clear reporting lines and ensure that any persons who may be implicated or conflicted in the matter are removed to avoid any potential conflicts or interference.

Addressing the desired outcome of the investigation early on is also important. Is the objective to stop/prevent misconduct, build a case for disciplinary, criminal, or civil action, or is it in response to a regulatory request? By preparing an initial investigation plan, you can better assess and justify the required budget and resources, which are often determined by the severity of the allegations and their financial and regulatory impact on the business.



2

PART TWO

PLANNING AN EFFECTIVE INTERNAL INVESTIGATION

Part 1 unpacked the '*What, When and Why*' of corporate investigations. As explained, corporate investigations are a vital part of healthy, functioning organisations.

An effective internal corporate investigation will ensure that an organisation is presented with relevant and accurate facts, which will allow for informed decision making. The type of investigation, and the resources allocated to resolving the issues identified, depend on the seriousness of conduct being investigated and its potential impact on organisation. The benefits of conducting an internal investigation are far-reaching:

- Investigations can uncover potential wrongdoing by management, employees or third parties and the malfeasance can be stopped before causing any further harm.
- It promotes a culture of accountability within an organisation and promotes awareness of potential risks.
- Investigations can uncover potential financial losses or claims that the organisation might have against third parties.
- Investigations serve to demonstrate to employees, counterparties, shareholders, regulators, financiers, insurers and investors that an organisation is serious about ethical conduct and "doing the right thing".
- The outcome or conclusion of an investigation can also potentially lead to a reduction in civil liability or pecuniary sanctions. Moreover, a company that self-reports to law enforcement, regulators and agencies, is likely to obtain recognition for doing so.

Although this section focuses on internal investigations (i.e. internally managed), it is important to note that organisations, in certain instances, may need to consider appointing an external investigation team to lead the investigation process. Such instances include:

- Where allegations relate to misconduct or negligence on the part of a member of the organisations executive or management team;
- The allegations being investigated may impact financial reporting or trigger a Reportable Irregularity;
- There is a likelihood that the alleged misconduct may lead to a criminal report or to third party litigation;
- The persons responsible for the internal investigation are potentially implicated in the conduct being investigated (e.g. managers, internal legal or audit committee members);
- The organisation does not have the necessary capabilities internally to conduct the investigation or external support may be required to recover financial losses; or
- When the matter may have, or is likely to attract media attention or regulatory scrutiny it is essential to have an independent and impartial investigation performed by appropriately qualified external experts appointed to establish the facts.

WHO WILL BE CONDUCTING THE INTERNAL INVESTIGATION?

Benjamin Franklin is quoted as having said that: '*failing to plan, is planning to fail.*'

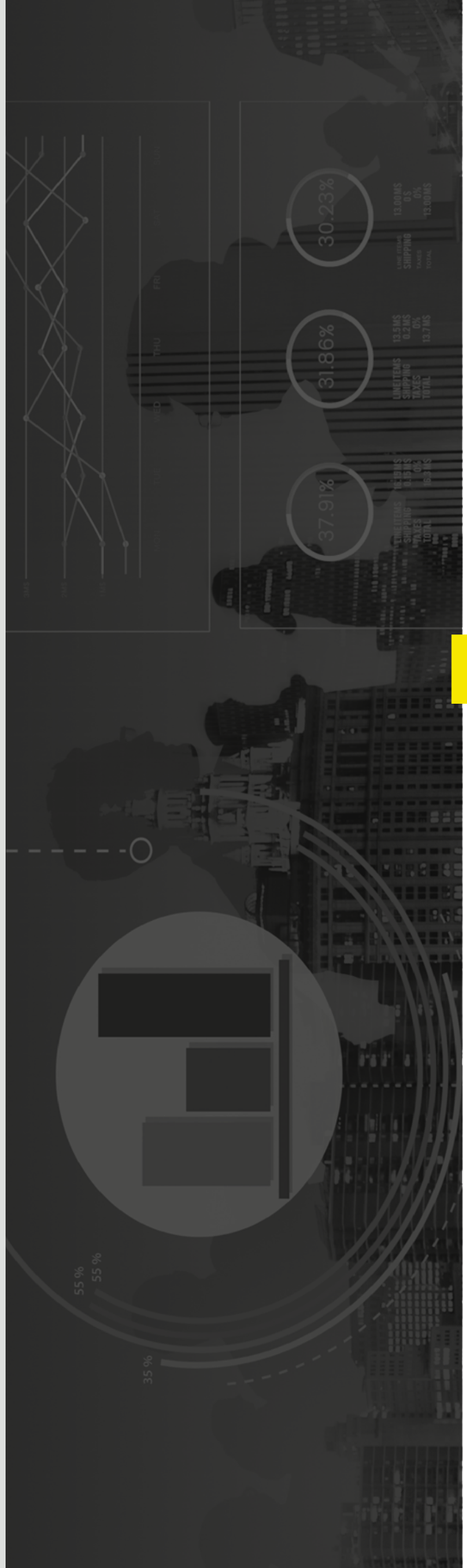
Once it is established that an internal investigation is necessary, the next step is deciding who will perform the investigation.

Organisations may have an internal investigation function or forensics team who are designated to conduct internal investigations. The investigation may also be performed by an organisation's compliance function or members of the internal audit team. Perhaps it's just an individual, a manager or 'jack of all trades', who is expected to get to the bottom of the issue.

Regardless of an organisation's structure, there are many ways to manage the investigation. Collaboration is key. Leadership, middle management, finance, procurement, IT, legal and HR, all have a part to play. Without compromising the confidentiality of the process, key individuals need to be identified and briefed on how they will support the investigation. Implicated persons also need to be managed and excluded from the investigation and evidence collection processes.

The possible stakeholders involved in conducting the internal investigation may include:

- **IT**: The IT team may need to extract digital data for assessment. Their involvement is essential to ensuring that data retention policies and preservation is carried out correctly – there is more to it than a 'copy and paste' of data. Information must be gathered in such a way that it is admissible in legal proceedings and must be done in a procedurally correct manner.
- **Finance and accounting:** Finance can provide important documentation which can help ascertain whether there is any merit to the allegations. Financial information (budgets, reports, purchase order information, invoices, general ledger entries) will help to identify trends, anomalies or financial misconduct.
- **Procurement:** Support from the procurement function of an organisation becomes essential when the investigation relates to procurement or third-party suppliers. Procurement can provide RFP specifications, tender response documents, procurement files and the on-boarding documentation which is invaluable to an investigation of this nature. Analysis of these documents may identify a deviation from (or circumvention of) company policy or standard operating procedures.
- **Legal:** Legal input in an investigation is necessary for a variety of reasons. This includes ensuring adherence to company policies, the collection of investigation and evidence, as well as overseeing engagement with employees and third parties. The legal team will also assist with any legal steps required in the remedial process following the completion of the investigation. Such steps would include, considering whether the incident has triggered a reporting obligation in terms of local and/or international law, disciplinary actions and litigation.
- **HR** : Internal investigations usually involve employees. HR therefore needs to be aware of the investigation from the outset. HR are also usually the custodians of employee disclosure information (when the concern suggests a conflict of interest) and other employee information relevant to the investigation. HR, in conjunction with legal, will also ensure that the employees' rights are adequately protected during the investigation. If the circumstances warrant, after consultation with management, HR may initiate and manage the suspension process and will arrange for company issued devices like cellular phones or laptops to be collected from the employee, for further assessment in advancement of the investigation. Finally, HR will support the consequence management steps and the remedial action plans (particularly those which relate to staff continuity), at the end of the investigation.



PLANNING THE INVESTIGATION

In the initial stages of the investigation, there is typically significant pressure on the investigator to report to leadership on the impact and severity of the allegations raised and to commence remedial action as soon as possible. However, jumping into an investigation without a proper investigation plan can be detrimental to the final outcome. Quick wins at the beginning of an investigation can lead to catastrophic failures later. We include below an example of some useful questions to ask when formulating an investigation plan.

ALLEGATIONS

Are the allegations against an employee or external parties?

Where was the offence / misconduct committed? Within a business unit / branch / jurisdiction?

Do the allegations have a financial impact? What is the potential prejudice to the organisation?

Do the allegations have a reputational impact? What can be done to manage the reputational damage or "get ahead" of public opinion?

Summarise and categorise the allegations into key concerns or types of misconduct:

- Does it relate to a criminal offence e.g. theft, fraud or corruption?
- Does it involve third parties or government officials?
- It is a procurement irregularity?
- Is it a conflict of interest issue?
- Does it relate to mismanagement, negligence or ethical misconduct
- Is it a failure to comply with company policy? What internal policies or Standard Operating Procedures may have been breached?

Assess the severity of the potential repercussions for the organisation. i.e. is there likely to be a statutory reporting obligation or a criminal matter? Will the outcome affect business partner relations, etc?

PERSON/S OF INTEREST	Is the source of the allegation known? Are they contactable to potentially provide further information? Is the suspect/s named in the allegations? Who does s/he report to? Who authorised/approved the transaction? If a supplier/service provider is alleged to be involved, who is the owner and/or representative of this entity? Who, internally, holds the relationship with the supplier? (Engaging with the Legal and Procurement functions (if it relates to a third-party supplier), may be critical even in the early stages of investigation.) Is the employee (person of interest) still a threat? Consider the impact of their existing access rights and / or influence on possible witnesses. Consider change of controls or suspension to prevent potential interference with witnesses or data or document compromises.
SUPPORTING FACTS	What do you already know and what evidence do you have to corroborate it? What additional facts do you need to fill the gaps? Where will you find this information?
SUPPORTING ROLE PLAYERS	Who do you already know that can provide further context around the allegations? Are they current employees, former employees, third parties, or friends of the person of interest? Prepare a list of custodians (individuals who hold information). Establish when and how you plan to approach them, taking into account the likelihood of potentially jeopardising the investigation versus the information they may hold to help you to proceed with the various stages of the investigation.
SOURCES OF INFORMATION	What preliminary steps can you take to covertly uncover additional information/evidence? E.g. can IT provide you with the emails? Or Finance with financial information, without alerting anyone else? Who is likely to have access to information which could substantiate or disprove the concerns?
ANTICIPATED GAPS OR LIMITATIONS	Where do you anticipate gaps or limitations to conduct or conclude the investigation? What hurdles and challenges do you foresee in verifying aspects of the allegation/s? Has an important witness moved overseas? Is surveillance footage still available or has it been overwritten? Are your policies in place to collect important data sources? Document the risks and possible mitigation steps and liaise with legal and IT early-on in the process.

Not all the information will be available at start of the investigation. Recording the known facts in a report format from the outset, will save time at the reporting phase. It will also help identify any gaps in the investigation and information.

As the understanding and scope of the investigation naturally evolves, it is critical to continuously assess the company policies, legal and reporting requirements, and to prioritise and reassign resources.

CONCLUSION

In this section, we highlighted the importance of planning and effective stakeholder management. The next part in this series will provide a detailed explanation on how to execute a fit for purpose and legally defensible internal investigation, with a particular focus on gathering and analysing evidence, and other data related aspects of an investigation.

We detail the importance of data in internal investigations, specifically, data preservation, extraction, retention and best practice.

3 PART THREE

CONDUCTING AN EFFECTIVE DATA REVIEW

After establishing that an internal investigation is necessary, this part in our series deals with the possible stakeholders involved in an internal investigation. It also refers to the necessary processes for planning an effective investigation. In part 3, we look at the more nuanced aspects of internal investigations, and specifically the process of obtaining and analysing relevant information and evidence. We also provide guidance in terms of best practice and industry standards.

INTRODUCTION TO DATA REVIEW

One of the key elements of an investigation is the collection and analysis of information, which is often colloquially referred to as the “data review”. The data review entails the systematic collection and review of information. Although it may appear straightforward, the data review process in internal investigations is frequently a complex undertaking. It involves gathering data from IT systems and email servers, navigating data protection regulations, and sifting through numerous business communications and computer files to pinpoint pertinent information. This task poses significant challenges. A thorough and efficient data review enables investigators to gain a clear understanding of the facts and plays a pivotal role in uncovering the truth. Often the data review will identify critical evidence, the proverbial “smoking gun”, which may prove either guilt or innocence.

Data reviews are essential for conducting reasonable and legally defensible internal investigations. Failure to complete a proper data review may result in regulators, law enforcement agencies, and even your own auditing firm perceiving the investigative process as inadequate or flawed.

In order to conduct a successful data review, one first needs to understand the different types of information available for review. In this part of the series, we simplify the different categories of information and provide examples on how they speak to one another and their significance in the investigation process, bearing in mind that this is not an exhaustive list. Considering the fast-paced technologically driven world, the kinds of data that is seen during the course of an investigation, is ever evolving (E.g. cryptocurrency transaction data, AI generated data, complex ownership structure data and various schemes to launder money).

The principle of an effective data review process lies in considering all the available information and being able to analyse complex and unusual data from different sources. This approach enables a comprehensive understanding of the data within its relevant context and facilitates swift analysis.

It is crucial to be aware of the pitfalls associated with trying to analyse large amounts of data from different sources. One such pitfall is the fact that not all data is text searchable, e.g. scanned PDF documents. The use of eDiscovery tools can greatly aid a data review through the use of OCR (optical character recognition) software and other mechanisms which allow for the easy categorisation and comparison of data across different types of information.

INTERNAL INVESTIGATIONS AND DATA

Preserve widely, process conservatively. Once a particular type of data has been identified for analysis and review, the data needs to be filtered and irrelevant information discerned from the relevant information. It is not

recommended to filter electronic data on internal systems, for example running search terms across Windows Explorer or an email archival system because the search function parameters differ from system to system. If it is required, this process should be conducted with the involvement of qualified personnel to ensure that the filtering process is done correctly and properly recorded.

The key focus for an efficient review is to structure unstructured data. It saves time and is cost-efficient to incorporate specific types of data together. For example, an eDiscovery platform can structure hard-copy and electronic documents like agreements, purchase orders, invoices, policies, etc, systems data, emails, corporate chat messages, BYOD chat messages (e.g. WhatsApp) and meeting recording transcripts into a format that allows for advanced searching and review, in context, together. Often, conversations of interest start formally on corporate-approved channels such as, financial accounting system data, documents, emails, and migrate to other devices, such as, WhatsApp's, conference call transcripts and Teams' chats.

If the investigation is performed by a team, determine the appropriate personnel and process for completing the data review as efficiently and cost-effectively as possible. Where different people are performing different parts of the analysis and review, a plan should be in place with the objectives of testing and reporting on findings to create a collaborative and non-duplicating team environment. A data review should develop the factual foundation of what happened. The picture will be made clearer when combined with the review of other information and feedback from witness interviews.

DIGITAL INVESTIGATION / INFORMATION INTERROGATION (DIGITAL FORENSICS)

Digital forensics is the term used to depict the application of scientific and technical procedures to preserve, validate, identify, extract, analyse, interpret and document evidence obtained from digital sources. In other words, it is the investigation of electronic devices, computers, laptops, mobile phones, email servers, file servers, handheld devices, memory cards, hard drives or any type of digital media believed to be used in various activities, particularly illegal or unauthorised activities.

Digital Forensics is carried out with the purpose of determining relevant information such as what transpired, when it occurred, where it took place, how it happened and who was involved or affected. It may also concern the decryption of password-protected files, identification of hidden information or the recovery of deleted files.

A typical case for Digital Forensics in an internal investigation is to identify when someone copied information from a network folder to a portable hard drive or flash memory device, which is often hidden or deleted. For example, tools have been developed to scan exiting employees' laptops to identify whether Intellectual Property has been copied or shared. Digital Forensics can be a discrete task and should be performed by a digital forensic expert. There is an overlap between Digital Forensics and eDiscovery which is outlined below. For example, where the recovered information, purportedly leaked, requires review by the investigation team, the Digital Forensic expert will provide the leaked documents to an eDiscovery expert to prepare for review by the investigation team.

The outcome of an internal investigation often hinges on the admissibility of evidence. Engaging a qualified digital forensic expert ensures that crucial digital evidence is properly collected and admissible in legal proceedings. The findings of the digital forensic investigation must be based upon scientifically established methodology and techniques and ought to be replicable. This means that another digital forensic examiner should have the ability to duplicate the examination and yield the same results. The process followed to recover the information can be interrogated during the legal proceedings. For example, if the evidence that a party seeks to rely upon was obtained through the recovery of information on a laptop and it is contested in court, the admissibility of the evidence will be in question if the person performing the process was not sufficiently qualified or the findings are not replicable by another digital forensic examiner.

It is important to note that holding IT qualifications is not the same as being a qualified digital forensic expert.

ELECTRONICALLY STORED INFORMATION REVIEW (EDISCOVERY)

Digital Forensics often relates to a discrete task on a specific type of device, whereas eDiscovery tends to connect multiple tasks and Electronically Stored Information ("ESI") together. ESI encompasses any documents or information that is stored in electronic format. The main types of ESI in internal investigations includes Microsoft Office Documents, Emails, Chat Messages, Collaboration Tool Data, Audio, Video and Social Media data. These file types are often located in the cloud, on laptops, computer hard drives, mobile devices (phones and tablets), corporate network servers, storage devices, such as, USB drives, and the internet.

In contrast to Digital Forensics, the role of eDiscovery experts is often not to find evidence per se, but rather to make it easy for the investigating team to find and review the evidence. On larger matters, eDiscovery experts can manage and formulate a structured review plan and, if required, provide large cost effective review teams to assist with the review of information. eDiscovery experts have been implementing technology-driven methodologies, including machine learning and other applications of artificial intelligence (AI), for many years. eDiscovery experts will integrate AI and automation to create the most efficient and cost effective data review possible. The recent explosion of generative AI provides an additional layer of search functionality.

Often, an auditor or regulatory body will interrogate the process followed during the investigation. eDiscovery experts provide a defensible, audit trail documenting the whole process, from preservation of the data through to production of evidence, throughout the investigation. eDiscovery experts will keep a log of all data preserved, seized and collected in order to maintain chain of custody records. The log needs to include details on who carried out the different processes, when they were carried out, and record any particular data exceptions and exclusions. The logs should also include the size of the data and how many documents were extracted/accessed. An eDiscovery document review platform will track all user activity during the preparation of the documents as well as the analysis and review itself. When an investigation ends, the data alongside the review details can be archived. Should the investigation become active again, the matter can be resumed in the eDiscovery platform with all of the review details and data from the date that it was archived.

It is important to note that there is an obligation to conduct this type of an investigation in a manner that preserves the integrity and veracity of the data, adheres to rules of evidence and chain of custody, considers data privacy implications and observes legal procedures and processes.

HARDCOPY INFORMATION REVIEW (EDISCOVERY)

Despite the digital age we live in, there are still a number of investigations requiring the review of paper and hardcopy documents. The manual review of hardcopy documents is rife with potential issues, including but certainly not limited to, accidental destruction of the original evidence through, for example, a coffee spillage. eDiscovery technologies can assist in digitising hardcopy documents and converting it to a searchable format to be reviewed alongside other ESI, in context.

As with all data in an investigation, chain of custody plays an important role for knowing who was in possession of the data. A proper chain of custody record is essential if the data is to be used as evidence in Court. Typically, the chain of custody records of hard copy documents can be established through the use of bar codes or other tracking mechanisms that attach a unique identifier to each page of the document. That identifier then links back to the source, origin and authenticity of the document. Taking photographs and videos of the hardcopy documents is also advisable as a means to confirm authenticity. The original hardcopy files should also be stored securely for preservation purposes.

FINANCIAL INFORMATION ANALYSIS (DATA ANALYTICS)

Depending on the nature and complexity of the transactions being investigated, specialists (most notably, chartered accountants, data analysts and financial experts) may be required to review and make sense of the data.

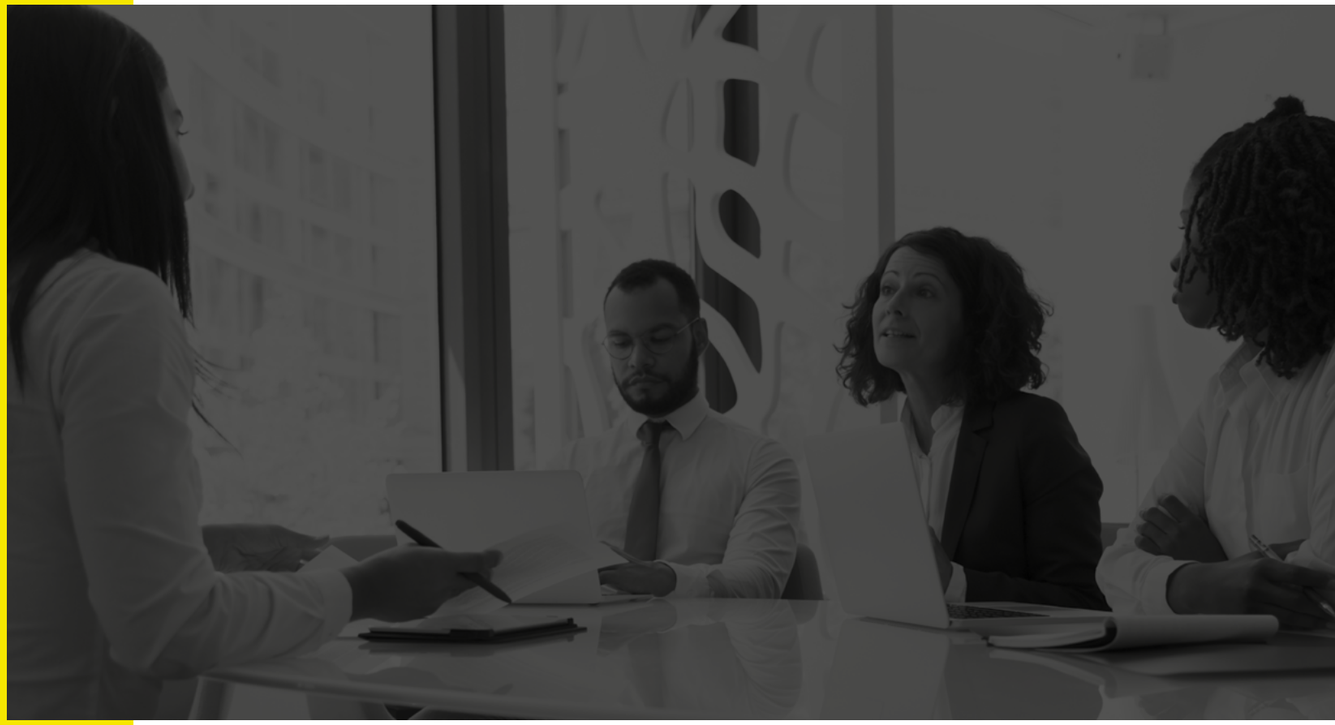
Analysis of financial data should be combined with ESI review and should not be performed in isolation. When a potentially fraudulent transaction is identified, it is imperative to search the ESI, which may provide an explanation or give context to the transaction. A good starting point is looking at conversations and correspondence taking place around the same time as the transaction. Often the ESI will serve to substantiate or refute the allegation. The analysis of the ESI will also help uncover any gaps or loopholes in the business processes.

CONCLUSION

Part 3 in our series has explained the significance of data and how it should be analysed in order to execute a quality internal investigation. In part 4, we explain how combining data and the evidence gathered during the investigation, with an effective interview process, can secure a successful outcome.

4 PART FOUR

CONDUCTING AN EFFECTIVE INTERVIEW - THE LINK BETWEEN DATA REVIEW FINDINGS AND INTERVIEWS.



The age-old question of 'What came first, the chicken or the egg?' is an appropriate adage to ascribe to this next section of our five-part series. When it comes to forensic investigation, the question is 'What comes first, the data review or the interview?'. Whilst no investigation is complete without either, there is certainly a synergy between the two processes.

Highlighted below are several best practices and pitfalls to avoid when preparing for and conducting interviews. Given the complexity and nuance of this topic, we categorise our advice and guidance into the three key phases of the interview process, namely:

- pre-interview (preparation),
- during the interview,
- and post the interview.

PREPARATION FOR INTERVIEWS

Early Case Assessment (i.e. using advanced searching techniques to quickly identify facts and key information) will help the investigation develop a dramatis personae (cast of characters) as well as assess the severity and scope of the matter.

A review of documents and communications can also help determine your witness list and identify further potential sources of evidence for preservation. eDiscovery technologies provide visualisation tools and analytics to quickly show who was party to certain discussions and correspondence. It can also assist with the rapid isolation and review of communication between specific individuals, and build visual timelines of events.

A review of financial data can help pinpoint the date ranges of particular interest. For example, if a potentially fraudulent transaction took place in June 2022 then the data under review can be filtered appropriately to see only the communications that occurred around the time of the fraud. The information obtained during the data review can then be presented and/or tested during the interview process.

When considering who should be interviewed, remember that an interview will likely result in the witness becoming aware of the investigation and the topics under investigation. This should be taken into account when deciding the order of the interviewees, how much notice (if any) to provide an interviewee and where to conduct the interviews.

Depending on the kind of witness interview, the interviewer may wish to provide guidance on the process to the interviewee and try make them feel comfortable with the process. By impressing upon interviewee the need for confidentiality and their ongoing cooperation, they may be inclined to cooperate. This is valuable at the outset of an investigation as, at this stage of the process, they likely know more than you and have access to the information you need.

For the suspect or 'defensive' interviews, your approach may need to be revised. At the very minimum, due process protocols should be followed.

DURING INTERVIEWS

The benefit of conducting a limited data review in advance of a witness interviews is that you are able to get a better understanding of the facts of the matter and can use that information during the interview process. The facts and events at issue can be discussed with the witness during the course of their interview. This can help identify whether the witness is a friendly witness (their statements are corroborated by the review) or whether you need to tread more carefully (there are inconsistencies between the witnesses assertions and the findings of the review).

Having an initial understanding of the facts can also help trigger a more accurate recollection of events from the witness. Similarly, inconsistencies in a witness's testimony can also be identified much easier, if you already have a grasp of the facts and timeline of events. A witness's memory is also not always accurate and thus having the fact pattern in advance of an interview can assist with correcting any memory lapses. Some other helpful hints are included below.

- Keep the interviews serious and businesslike. An interview is no place for joking, sarcasm or threats.
- Interview only one person at a time. It is ill advisable to interview groups of people at the same time. Group dynamics and peer pressure may distort or suppress responses.
- Never stoop to undignified tactics. At times, you may need to be aggressive or tenacious, but never insulting or demeaning. Intuition is to be used in this regard within the necessary boundaries.
- Use technology to have evidence at your fingertips during the interview (e.g. if the interviewee refutes or claims – pull up the evidence for/against it before the interview ends).
- Be cognizant of any colloquial language or nicknames used by the witness to refine your search criteria across the communication data.
- Never mislead a witness. This will result in employees distrusting the entire process.
- Do not tell the witness what other witnesses had to say. You do not want the witness to conform his or her statements to the statements of others. Do not discuss your opinions or conclusions.
- Do not expect an admission in an interview. The investigation should focus instead on eliciting as much relevant information as possible.

It is also imperative to keep a proper record of the interview and what was discussed. This may entail detailed notes of the interview or a recording. If notes are prepared at the conclusion of the interview, it is advisable to do so as soon as possible, while your recollection of the interview is fresh.

POST INTERVIEWS

After individual interviews or the interview stage has completed, you should have a much better understanding of who was involved in the incident / irregularity. If you recorded the interview, get it transcribed (but get your CIO or IT Officer's input regarding the platform or third party transcription provider, as you may be transferring potentially personal information to different jurisdictions).

Consolidate your interview notes and identify where various witness testimonies are corroborated by other witnesses or documentary evidence. Also look for gaps in witnesses testimonies as this will inform the next steps of the process (i.e. is further data review, or interviews required).

If all available data has been reviewed and all relevant interviews have been conducted and you still have an inconclusive finding, you may need to get creative. Depending on the nature of the allegations, there may be other tools and processes in an investigator's armoury, which could help plug the gaps and reach a more conclusive finding. These include:

- Polygraph assessments

  In South Africa there is currently no legislation regulating the use of the polygraph. It would, however, be against the Constitution of South Africa to compel a person to undergo a polygraph examination, he/she must consent to the process. Notwithstanding, polygraph assessments can be a helpful investigative tool. It is important to remember that a negative outcome of the polygraph (i.e. deception indicated) on its own is not enough to dismiss an employee. We advise obtaining appropriate employment law advice in such circumstances.

- Bank statement analysis

  There is nothing wrong with asking a suspect employee if they would be willing to provide their bank statements for review. This would primarily be to ensure that there are no suspicious money flows in or out of their accounts, which may be evidence of collusion or corruption.

We caution that these processes can be perceived as very invasive. Consideration must therefore be given to the way you broach these requests with the person of interest. You may wish to involve an external service provider to handle these processes delicately. The limitations, benefits and risks of each process need to be weighed up before each process is carried out.

CONCLUDING AN INVESTIGATION

A defensible investigation requires an auditable methodology and a report setting out the investigation steps taken. Such a report should include detail on quality controls regarding the preservation and review of data, and the production of evidence. Such steps not only enhances and safe-guards the reliability of the evidence identified but also ensures that the evidence is admissible in any legal processes that may follow the investigation.

The most paramount part of any investigation is summarising the facts gathered throughout the investigation into a report. This is often a time consuming and sometimes overwhelming task. It doesn't have to be. In essence, the final investigation report should state whether the concern / allegations were substantiated, unsubstantiated, or that the findings were inconclusive. The key evidence supporting your conclusion must be included in the report and should be set out in a concise and logical manner.

There is benefit to linking the evidence (facts, people and events) in a visual timeline. This, together with a succinct written report can be a valuable aid for organisations to develop corrective procedures to avoid repetitions of questionable conduct. This form of reporting can also be a persuasive way of communicating to third parties that (1) wrongful conduct did not occur, or (2) that corrective action has been taken internally, if it did.

Alternatively, a comprehensive written report might be necessary to satisfy your external auditors, particularly if a Reportable Irregularity is suspected. The report should be fact-based and supported by exhibits or attachments that would supplement the findings of the review. The report will need to establish (1) whether the wrong-doing is material, (2) if the wrong-doing is on-going and (3) whether management has demonstrated the level of responsiveness expected of ethical and transparent leaders.

It should also be borne in mind that if the allegations are substantiated the investigation may also trigger:

1. disciplinary action against an employee or other remedial actions such as counselling or professional assessment of an employee, mediation between employees and possibly the termination of an employee. [A future article in this series will focus on corrective action from an employment law perspective];
2. the severing of relationship with a service provider as a result of a breach of contract;
3. a reporting obligation in terms of Section 34 of the Prevention and Combating of Corrupt Activities Act, 2004 (PRECCA), which places a duty on defined persons in a position of authority (i.e. director, manager, Chief Executive Officer) to report certain offences over R100,000;
4. the opening of a criminal complaint; and/or
5. the launching of civil proceedings.

IN CLOSING

By conducting an internal investigation efficiently and applying the same defensible and repeatable processes across future investigations, you will significantly reduce the burden on your team.

This section has explored how an effective internal investigation is carried out and demonstrates what the planning and executing of a quality internal investigation entails. As the series continues, we unpack the formulae of a sound and effective corporate investigation strategy, the weeks to follow will focus on (1) how to conduct an effective email review, (2) QC and external digital support, (3) data privacy considerations, (4) employment law support and (5) continuous monitoring and information governance.

5 PART FIVE

HOW TO MAKE THE MOST OF EXTERNAL SUPPORT IN AN INTERNAL INVESTIGATION

In Part 2 | How to plan for an effective internal investigation), we pointed out instances when an external (independent) investigator may be required. There are a variety of reasons why the assistance of an external, independent third party may be required to assist with an internal investigation.

Outsourcing a portion, if not the entirety, of an investigation is driven by key factors such as efficiency, defensibility, objectivity, reliability, and the quality of the resulting evidence. This is especially crucial when allegations involve misconduct or negligence by a member of the executive team, who might ordinarily be involved in initiating the investigation. Outsourcing ensures objectivity and defensibility, as it can be challenging for an employee to maintain objectivity while investigating their senior colleagues. This challenge could potentially cause irreversible damage to relationships, particularly during the interview phase, negatively impacting the prospects of the internal investigation team.

The following are just some examples of instances where it may be useful to outsource a portion of an investigation:

WHY WOULD YOU OUTSOURCE YOUR INVESTIGATION AND INVOLVE AN INDEPENDENT THIRD-PARTY

- In situations where there's a potential impact on financial reporting or the possibility of triggering a Reportable Irregularity, your audit firm might mandate an external investigation. Time sensitivity, especially near the financial year-end, underscores the importance of promptly outsourcing to an independent third party when such allegations arise. The consequences can be significant; for instance, your auditors may hesitate to endorse your financial statements on time, or at all, leading to detrimental effects on the business's reputation and finances. This may result in diminished investor and lender confidence, potential liquidation proceedings, and, if applicable, delisting.
- In cases where there's a potential to recover a financial loss suffered by the business, be it through asset recovery, an insurance claim, or the pursuit of civil remedies, solid evidence of fraud is crucial. Independent experts like forensic accountants may need to be brought in to document and quantify the loss.
- When there's a high likelihood that alleged misconduct could result in a criminal report or litigation, gathering evidence becomes pivotal for a successful conviction or litigation. If data is not appropriately collected from the outset, the reliability of the evidence can be easily contested, potentially causing the entire case to unravel. Failing to do so may lead to wasted time, energy, and costs in the court process, rendering losses from the misconduct unrecoverable and holding those leading the investigation accountable.
- Cases that demand time and effort beyond your internal resources or expertise should be considered for outsourcing. Failing to handle misconduct appropriately and swiftly can establish a toxic culture within the organization.
- Where situations garner media attention or regulatory involvement, the investigation requires a demonstration of impartiality and independence.

WHO, WHEN AND HOW TO DECIDE TO OUTSOURCE YOUR INVESTIGATION

When confronted with a situation that warrants an investigation, an organisation and its management need to determine whether the investigation requires or would benefit from being outsourced to an external forensic, digital forensic and/or eDiscovery provider. It is therefore necessary to conduct a risk assessment of your in-house resources, skills and capacity.

It is important to understand the implications of the allegations, the type of external support that can be provided as well as the specialist skills required for certain types of allegations and investigatory activities.

OUTSOURCING VERSUS INTERNAL RECRUITMENT AND TRAINING COSTS

You may need to bring in specialist skills for different types of investigations. For example:

- If the investigation may violate the Foreign Corrupt Practices Act (FCPA) then you should seek a forensic practitioner with seasoned experience in dealing with FCPA matters and quickly.
- If the investigation requires a comprehensive financial analysis, you may need a chartered accountant or data analytics specialist. You might not have access to these on a full-time basis, so it is important to build a trusted relationship with a provider that can provide these specialist skills on an hourly-charged basis.
- You will need the expertise of a digital forensic expert to 'image' a laptop or cellular device in a forensically sound manner, to preserve and retrieve all available data.
- An objective interviewer can elicit more information and will avoid later questions of unfairness or undue influence when, say, a more senior in-house resource interviews the witnesses or suspects.
- Technology-driven methodologies will drive down the number of people you need in a team. This is particularly important when there is high staff turnover due to the pressures on the compliance team. There are many ways to bring technology into your

department. Digital forensic and eDiscovery software licensing often require large upfront investments, upgrading and maintenance and training to keep running. If your investigations don't involve handling substantial amounts of data regularly, outsourcing to a provider with the expertise, processes, and legal technology to seamlessly manage data—from collection to review and the production of credible evidence—often proves to be the most cost-effective choice. Alternatively, you can request a self-service option where your team runs the projects on their licensed platforms on a pay-as-you-use basis.

- In cases where a significant amount of information needs to be reviewed, cost-effective managed review teams are available to sift through the information to provide all the relevant documents (and excluding irrelevant ones) to the investigation team.
- Cross-border matters require legal and data privacy experts who have built an extensive knowledge base, along with a profound understanding of local nuances and business practices in particular regions.

CONCLUSION

Corruption is a global challenge, and Africa is no exception. Of the 2,110 occupational fraud cases from 133 countries analysed by the 2022 ACFE State of the Nation report, Sub-Saharan Africa made up 23% of these cases (429 cases). To give further perspective to these issues, Certified Fraud Examiners estimate that organisations lose approximately 5% of revenue to fraud each year. Investing in proper legal and forensic support is crucial to combat fraud and corruption effectively.

Should you require external legal and forensic support, ENS is well-equipped to provide proper guidance. Our distinguished team comprising highly-skilled and award-winning professionals including accountants, investigators, digital forensic experts, data analysts and fraud prosecutors, collaborates seamlessly with our state-of-the-art digital platforms providing you with comprehensive solutions suited to your company specifics.

ENS'S CORPORATE INVESTIGATIONS TEAM IS HIGHLY REGARDED FOR ITS ABILITY TO HANDLE SIGNIFICANT FORENSIC INVESTIGATIONS, WITH PARTICULAR PROFICIENCY IN COMMERCIAL CRIME INVESTIGATIONS AND ANTI-CORRUPTION CONCERNS

CHAMBERS GLOBAL GUIDE

CONTRIBUTERS

STEVEN POWELL
HEAD | FORENSICS

CANDACE LATEGAN
FORENSICS MANAGER

LINDA SHEEHAN
HEAD | intelligENS

ANDREW KEIGHTLEY-SMITH
SENIOR ASSOCIATE | FORENSICS

COLETA WESSO
ATTORNEY | intelligENS