



Lifestyle audits and fraud prevention: Elevating HR's role in combating white-collar crime

Working paper series

WP/2025/02



This document is intended for public use. It may be distributed without the permission of the Centre of Excellence in Financial Services, as long as reference and credit are given to the authors when cited.

The Centre of Excellence in Financial Services is a non-profit organization focusing on collaborative research, bringing together local and international thought leaders, industry experts and academics to interrogate the role financial services can play in achieving national and international objectives. This working paper is available in electronic format on www.coefs.org.za.



Table of contents

Preface	ii
Members of the work group	iii
Abbreviations	iv
Executive summary	v
Background and context	1
Introduction	4
Understanding white-collar crime in South Africa	5
The current role of risk management in lifestyle audits	15
The case for HR – Led lifestyle audits	18
A human-centres framework for lifestyle audits	22
Corruption and the law	25
Institutional collaboration	28
Evaluating the current lifestyle audit and declaration of interest system ..	31
SA lifestyle audit and fraud prevention: gaps and global benchmarks	35
Conclusion	40
Bibliography	42

Preface

South Africa has struggled with its image as a leading jurisdiction for economic crime, with little effort being made to reverse this perception. The most significant enabler of change was the Financial Action Task Force (FATF) greylisting of South Africa in February 2023, for perceived weaknesses in its ability to effectively prevent anti-money laundering and combating of the financing of terrorism.

The Zondo Commission of enquiry report, which was finalised in June of 2022, provided sufficient evidence for one of the FATF concerns, the lack of prosecutions of complex financial crimes.

While South Africa takes action to curate its new image, we wanted to explore lifestyle audits as a means of stabilising this progress.

The digitalisation of everything has provided such an opportunity, and the desire of government to digitise public infrastructure and share data, combined with access to private sector data pools, the traditional approach of looking for answers once the crime has been committed could be transferred into a real time, on demand evaluation, of an individual's financial health.

We propose that financial crime is not just a risk discussion, it is more suited to a human resources discussion supported by risk, and that is how we have positioned this paper.

Active conflict of interest management, rather than a simple declaration, can be a leading indicator of potential fraud, and with ultimate beneficial ownership of companies receiving attention, proactive environmental scanning will become possible.

Mark Brits
Executive Director



Members of the working group

in alphabetical order

Siham Boda

Director
Corporate Insights

Mark Brits

Committee Chair
Executive Director
Centre of Excellence in Financial
Services

Pearl Masondo

Research Administrator
Centre of Excellence in Financial Services

George Nicholls

Chief Technical Officer
Corporate Insights

Members of the work group participate in their personal capacities, without remuneration, and their views do not necessarily represent those of their employer.



Abbreviations

Auditor-General of South Africa	AGSA
Financial Action Task Force	FATF
Protection of Personal Information Act	POPIA
Senior Management Service	SMS
Special Investigation Unit	SIU



Executive summary

White-collar crime, defined as financially motivated offenses committed by individuals in positions of trust¹, continues to erode South Africa's public and private institutions. From high profile scandals such as VBS Bank, Steinhoff, and the state capture of government, to more subtle instances of internal fraud, the impact is evidenced by billions of rands in financial losses, weakened institutional capacity, and a deep erosion of public trust.

This working paper introduces a digital approach, using lifestyle audits, to identify not only potential fraud, but omissions in declarations of interest, an important indicator of potential risk, and calls for a shift in the way lifestyle audits are understood and applied. Traditionally managed by risk or audit departments, lifestyle audits are typically reactive and investigative in nature. They are often triggered only after a financial loss has occurred, limiting their usefulness as a preventative tool.

We propose the repositioning lifestyle audits as a strategic, forward-looking function led by human resources (**HR**) and or finance professionals rather than solely risk and forensic practitioners. With regular engagements on employee behaviour, performance data, and wellbeing indicators, HR is uniquely positioned to detect ethical and financial risks early. By integrating lifestyle audits into existing HR processes such as onboarding, performance reviews, and wellness programmes, organisations can uncover vulnerabilities early, offer support, and foster a culture rooted in integrity and accountability.

Key insights from this report include:

TRADITIONAL audits often occur too late, missing early signs of financial stress or behavioural change. They are largely reliant upon manual processes and thus are comparatively costly to undertake.

¹ Corporate Financial Institute (CFI)



HR LED lifestyle monitoring enables proactive risk detection through continuous engagement and trust-based interactions.

REAL WORLD case studies highlight critical failures in oversight, control systems, and ethical governance, which is largely preventative.

INTERNATIONAL examples from Singapore, Estonia, and the United Kingdom show the effectiveness of digitised declarations, data integration, and institutional coordination.

SOUTH AFRICA's current framework is constrained by limited legal authority, fragmented oversight, and a lack of real time data access.

The report concludes by urging organisations to place lifestyle audit responsibilities within HR, complimented by the risk function, not to weaken them, but to enhance their strategic, ethical, and preventative impact. This shift is not simply procedural. It represents a cultural transformation that prioritises prevention over punishment, supports ethical decision making, and builds institutional resilience across sectors.



Background and context

Understanding the value of money begins when children are taught the difference between a person's needs and their wants, which is then linked to the delayed gratification of saving to conceptualise wealth. But, without a strong moral compass, when the opportunity arises to leapfrog through Maslow's hierarchy of needs, from the physiological to self-actualisation, some people will take the chance, as the financial rewards of some magnitude will seem unlikely and illusive over their lifetime. Potentially emboldened by the perceived chance of not being caught and if caught, not being brought to book, and a criminal justice system that is unable to materially shape societies moral consciousness.

South Africa has been challenged by an unacceptably high level of corruption, with the Judicial Commission of Inquiry into Allegations of State Capture, Corruption, and Fraud in the Public Sector, known as the Zondo Commission and colloquially referred to as state capture, describing "it as pervasive and deeply entrenched"².

The State was not alone in capturing the attentions of the public. Corporate failures like Steinhoff and VBS Bank, demonstrated that corruption and fraud were entrenched in our society. Race, gender, age, socio-economic background are not obvious parameters. A culture of entitlement, from bribes extracted by traffic police officers – an opportunistic crime, to identity theft and mobile phone sim swaps – a syndicated crime, have been normalised.

When those that have money are the victims, such as the government, companies or the wealthy individual, there may be less empathy, but as Corruption Watch explains:

"Corruption affects us all. It threatens sustainable economic development, ethical values and justice; it destabilises our society and endangers the rule of law. It undermines the institutions and values of our democracy. But because public

² Zondo Commission Reports



policies and public resources are largely beneficial to poor people, it is they who suffer the harmful effects of corruption most grievously.”

The Zondo Commission became the clarion call for accountability in government, and the former president Mr Jacob Zuma was jailed by the Constitutional Court for refusing to testify on his stewardship of the country during the height of this corruption. Within days, rioting and looting broke out in KwaZulu Natal that resulted in many deaths and a substantial financial loss to the economy.

The evidence provided by the Zondo Commission has demonstrated not only how corruption has damaged our country, but that prosecuting guilty parties may be difficult and politically costly. The Zondo report was damaging, creating the burning platform that would force government into action.

The Financial Action Task Force (**FATF**) in its Mutual Evaluation Report of South Africa, in October 2021, noted in its key findings that:

“South Africa has achieved some good results proactively pursuing confiscation of criminal proceeds, particularly using civil forfeiture powers but has had less success recovering assets from “State capture” and proceeds which have been moved to other countries. Some recent cases suggest that this situation is improving.”

However, this report would lead to the grey listing of South Africa in February 2023 and within its recommendations to strengthen the combating of money laundering, terrorist financing and proliferation financing, the Zondo Commission report would become more relevant and urgent to address, as South Africa faced higher scrutiny in cross-border transactions providing an additional cost to an already underperforming economy.

As part of the remedial actions to be taken by the government, key focus areas became the strengthening of law enforcement and to increase the number of prosecutions, particularly high-profile cases, and recovering the proceeds from these illicit activities.



The extradition of two of the Gupta brothers from the United Arab Emirates to face charges of fraud and corruption, failed in April 2023, apparently due to a technicality. The Zondo Commission presented a damning report into the relationship between the president and the Gupta family and for the prosecution of high-profile cases to become a reality, this extradition was a key element.

Reaction to the Zondo Commission recommendations has been slow. From the July 2025 progress report³, three years after the finalisation of the Commission report, of the 60 actions identified, 29 (48%) were considered complete or substantially complete, 14 (23%) were described as “on track” while 17 (29%) were delayed or requiring attention. Asset recoveries have reached R10.932 billion.

³ Progress report on implementation of actions in the president’s response to the recommendations of the state capture commission



Introduction

White-collar crime, typically referred to as non-violent, financially motivated offenses committed by individuals in positions of trust and authority, continues to siphon billions from South Africa's public and private institutions, weakening organisational performance and eroding stakeholder trust (Sutherland, 1983). Traditional responses - led by risk, audit, or compliance—have proven to be largely ineffective. These functions tend to activate only after misconduct occurs, leaving organisations unnecessarily exposed and vulnerable. Additionally, a sampling approach is undertaken which by purpose leaves parts of the organisation unevaluated. Where evaluation does take place, it is normally on areas of perceived risk, rather than areas where risks occur.

Among the tools used in fraud detection, lifestyle audits have gained recognition for their ability to identify discrepancies between an employee's declared income and observable wealth or spending patterns. However, they are still too often viewed as investigative or disciplinary measures, deployed only when suspicions arise.

This report challenges that model. It argues that human resources - with its visibility across the entire employment lifecycle - is better positioned to lead lifestyle audits as part of a broader ethics and wellbeing strategy. Through regular engagement, behavioural insights, and trust-based interactions, HR can help detect early risk indicators before they evolve into fraud, and engage with employees, offering support, while consulting with the risk departments to ensure vulnerabilities are appropriately monitored.

Drawing on real-world case studies, cost data, and an evaluation of current service offerings, the report proposes a reimagined framework for lifestyle audits: one that is preventative, ethical, and embedded in organisational culture. By shifting the centre of gravity from risk to HR, lifestyle audits can move from being a reactive control tool, to a proactive integrity safeguard.



Government has an important role to play if we are to be successful with lifestyle audits. Protection of personal information laws should be applicable to lifestyle audits but should not provide unintentional impediments for their use. Ultimate beneficial ownership of businesses is being proactively addressed, and the ability to gain access to this critical information, amongst others, in real time, will improve the value of lifestyle audits from a historical view to real-time.

Lifestyle audits must become a tool in the fight against financial crime and although universally applicable across both the public and private sectors, not all employees will be impacted. Designed to collect information, the risk can be proactively managed through HR where indebtedness, conflict of interest and financial distress can be addressed while naturally increasing the levels of compliance amongst staff and reducing the overall cost of compliance.



Understanding white-collar crime in South Africa

Common types of white-collar crime

White-collar crime in South Africa encompasses a range of non-violent offenses committed by individuals in professional or business settings for financial gain. The most prevalent types include:

FRAUD: Deliberate deception to secure unfair or unlawful financial benefits.

CORRUPTION: Abuse of entrusted power for private gain, often involving bribery or nepotism.

EMBEZZLEMENT: Misappropriation of funds placed in one's trust or belonging to one's employer.

MONEY LAUNDERING: Concealing the origins of illegally obtained money, typically by means of transfers involving foreign banks or legitimate businesses.

TAX EVASION: Illegal practices to avoid paying taxes owed.

CYBERCRIME: Criminal activities carried out using computers or the internet, including identity theft and online fraud.

These crimes are often facilitated by individuals in positions of trust and can have far-reaching impacts on organizations and the economy.

Sectoral hotspots: financial services and the public sector

White-collar crime significantly affects both the financial services and public sectors in South Africa:



Financial services sector:

Banks and financial institutions are frequent targets due to the large volumes of transactions and assets managed. Crimes include insider trading, fraudulent loan applications, and unauthorized fund transfers.

Public sector:

Government departments and state-owned enterprises often face issues like procurement fraud, misallocation of funds, and bribery. These activities undermine public trust and divert resources from essential services.

Case studies: real-world lessons from the banks, Zondo Commission, and others

Several notable cases have highlighted the extent of white-collar crime in South Africa:

Case study 1: Absa Bank – Internal staff fraud (R1 million)**What happened:**

Two Absa employees were convicted and sentenced to 15 years in prison for defrauding the bank of over R1 million between 2014 and 2016.

Fraud mechanism:

They exploited internal systems to divert funds into personal accounts, leveraging privileged access.

Detection method:

The fraud was not picked up through internal controls or lifestyle audits. It was discovered only after extended misuse and eventual escalation.

Key takeaway:

Routine lifestyle audits for system-access roles could have revealed sudden financial changes or asset accumulation, prompting earlier investigation and mitigation.



Case study 2: Standard Bank – Team Leader defrauds R3 million

What happened:

A team leader at Standard Bank stole over R3 million from client accounts, using their managerial access to mask the fraud.

Fraud mechanism:

The employee made unauthorised transfers from dormant or high-balance accounts to personal accounts and manipulated authorisation processes.

Detection method:

The fraud was detected only after significant losses had occurred, indicating failure of both transaction monitoring and behavioural oversight.

Key takeaway:

Ethics-based supervision and behavioural red-flag tracking are essential for mid-level and supervisory roles that operate with high trust and limited oversight.

Case study 3: R1.2 million scholarship fraud

What happened:

A senior executive formerly responsible for corporate social investment at a major South African bank was arrested for allegedly defrauding the Adopt a School Trust of over R1.2 million by redirecting funds intended for student bursaries.

Fraud mechanism:

She allegedly channelled money to relatives and shell companies, later receiving kickbacks into her personal account.

Detection method:

The fraud was uncovered via Standard Bank's internal review in 2022, followed by a formal Hawks investigation in 2024.

Key takeaway:

Even CSI and philanthropic units require independent audits and lifestyle monitoring of administrators who manage financial disbursements to ensure ethical governance.



Case study 4: VBS Mutual Bank – R2 billion “Great bank heist”

What happened:

Between 2015 and 2018, senior executives and associated parties orchestrated the looting of approximately R2 billion from VBS Mutual Bank, causing its collapse in 2018 and inflicting heavy losses on depositors—many of whom were ordinary citizens and municipalities

Fraud mechanism / lifestyle anomaly:

The fraud involved “cooking the books” - creating fictitious deposits and using suspense accounts to divert real funds into shell companies and personal accounts. Executives received excessive commissions, bonuses, and kickbacks, using public funds to finance luxury cars, properties, and upscale lifestyles.

Detection method:

The scheme came to light following a forensic probe ordered by the South African Reserve Bank in 2018, with investigative reports (e.g., “The Great Bank Heist”) uncovering the irregularities. Multiple arrests and prosecutions followed, though trials have faced delays and ongoing legal challenges

Key takeaway:

VBS is a textbook example of systemic failure across governance, auditing, and regulatory oversight. It underscores the need for real-time financial monitoring, independent audits, strict limits on perks and external fees, and oversight of public funds - especially when handled by mutual institutions.

Case study 5: Zondo Commission – state capture of SOEs

What happened:

Between 2010 and 2018, the Judicial Commission of Inquiry into Allegations of State Capture (Zondo Commission) revealed how high-ranking officials, including former President Zuma and the Gupta family, colluded to exploit state-owned enterprises (SOEs) - like Eskom, Transnet, Denel, Alexkor—for personal gain

Fraud mechanism / lifestyle anomaly:

Tactics included tender rigging, installation of compliant board members, unsanctioned supplier agreements (e.g. Gupta-linked firms), and opaque decision-making - all enabling officials to capture funds and bolster lavish lifestyles.

Detection method:

Detection was enabled through public hearings, forensic audits, and broad stakeholder submissions over nearly four years - culminating in a detailed multi-volume report by June 2022.

Key takeaway:

Large-scale fraud requires transparency in SOE governance, continuous forensic oversight, whistle blower protections, and active oversight of procurement and appointment processes - backed by lifestyle audits for those in strategic positions.



Case study 6: Steinhoff International – \$7.4 billion accounting fraud

What happened:

In December 2017, Steinhoff revealed a massive accounting irregularity: \$7.4 billion in fictitious assets recorded between 2009–2017. The market reacted violently, wiping over R200 billion (~95%) off its share price and triggering pension and investor losses.

Fraud mechanism / lifestyle anomaly:

Fraud involved bogus intercompany transactions, inflated earnings from fictional deals (e.g., Mattress Firm/Serta Simmons), and aggressive earnings management. Executives, including CEO Markus Jooste, benefited from false company performance.

Detection method:

An independent PwC forensic investigation (2018) uncovered the fraud; internal controls and auditors (e.g., Deloitte) failed to raise red flags - though JP Morgan analysts had earlier expressed suspicion in 2007.

Key takeaway:

Financial statement fraud can go undetected for years unless organisations have independent forensic reviews, robust auditor rotation, and continuous anomaly monitoring (e.g., unusual intercompany activity).

Case study 7: McKinsey & Company Africa – \$122 million bribery settlement

What happened:

In December 2024, McKinsey & Company reached a \$122 million settlement with U.S. and South African authorities over bribes paid by its African subsidiary (2012–2016) to officials at Transnet and Eskom - leading to over \$85 million in illicit profits.

Fraud mechanism / lifestyle anomaly:

The firm used confidential insider information and paid kickbacks via partner consulting firms to secure lucrative SOE contracts. A senior partner pleaded guilty under the U.S. FCPA.

Detection method:

The corruption was uncovered through a DOJ -led investigation, leveraging internal disclosures and foreign corruption laws. The settlement includes a Deferred Prosecution Agreement and compliance reforms.

Key takeaway:

Even top-tier global consultants must enforce stringent anti-corruption measures, including conflict-of-interest checks, partner vetting, and rigorous compliance training - especially when bidding for publicly funded SOE work.



Cross-cutting themes and lessons from the fraud case studies

Behavioural red flags were missed:

In nearly all cases - VBS, Absa, Standard Bank, McKinsey, Zondo-era SOEs - suspicious lifestyle changes or behavioural anomalies (e.g., lavish spending, quiet manipulation of systems, insider relationships, conflicts of interest) were visible but overlooked.

Lesson: Financial distress, lifestyles that do not accord with earnings, entitlement, or opportunity-driven behaviour are early signs that must be monitored continuously - preferably by HR in collaboration with Risk.

Internal controls failed or were circumvented

Steinhoff and VBS are glaring examples of internal audit or board oversight being either complicit, silenced, or technically outmanoeuvred.

In the Standard Bank and Absa cases, access control and segregation of duties were weak or ignored. Often times, data was not available to support conclusions drawn creating scepticism or opportunities and discount to overlook risk signals.

Lesson: Governance processes must go beyond checklists - ethical leadership, culture, and data transparency matter.

Lifestyle monitoring was absent or reactive:

In none of these cases were red flags evident through proactive lifestyle audits. Financial and asset anomalies emerged only after formal investigations.

Lesson: Systematic, continual, dignified lifestyle monitoring integrated across the employee lifecycle can serve as an early detection tool.

Whistleblowing worked—but came late:

Whistleblowers were critical in exposing fraud in VBS, Zondo Commission cases, and even parts of the McKinsey and Steinhoff scandals.



Lesson: Organisations must invest in safe, anonymous whistleblowing platforms - but also go a step further with preventative HR engagement to reduce reliance on crisis-stage tips.

HR management vs. risk management: complementary roles

HR Management	Risk Management
Expected to interact regularly with employees	Engages episodically, often post-event
Can detect behavioural red flags early	Relies on policy breaches and controls
Trusted to build relationships	Perceived as policing or compliance
Manages onboarding, ethics, wellbeing	Manages internal audits, controls
Can integrate ethics into culture	Focuses on detecting/reporting events

Implication:

Fraud prevention must become a shared function - not siloed in risk. HR must be trained and empowered to lead early detection and support mechanisms, while risk builds robust control frameworks.

Common loopholes across cases

Loophole	Examples
Lack of continual lifestyle or asset monitoring	Absa, Standard Bank, VBS
Poor whistleblower protection or uptake	Zondo Commission testimonies emerged years later
Weak control over third-party and vendor access. Lack of supportive data to underscore risk	McKinsey, SOE tenders, Steinhoff transactions
Insider collusion and override of processes	Steinhoff, VBS, SOE executives and board appointees
Absence of real-time financial surveillance	Steinhoff, VBS, Standard Bank internal systems
Ethics treated as a “soft” HR function. Risk treated in silo functions that misinterpret risk signals	All cases - where ethics were not central to hiring or performance culture

Strategic takeaway: from reactive to preventative

To prevent similar frauds in the future:

EMBEDED lifestyle continual audits into HR processes, not just for compliance, but as employee support and risk detection.

ALIGN HR and risk management, with shared dashboards, case triaging, and ethical intelligence tracking.



SHIFT from “*who broke the rules*” to “*where are the risks and how do we support ethical decisions?*”

These case studies highlight how white-collar crime, when left undetected, can escalate into scandals that damage not only individual organisations but also the broader economy. The next section explores the tangible financial and reputational costs of such misconduct.

Financial and reputational costs of employee fraud

The case studies presented in the previous section reveal how employee fraud - often concealed behind a façade of normalcy - can quietly erode organisational integrity and finances until it culminates in public discourse and reputational risk. These incidents underscore that often the event manifest over long periods of time without detection or using amounts that fall below thresholds. When misconduct goes undetected, the financial and reputational toll can be devastating. Below is a summary of the measurable costs of employee-driven white-collar crime in South Africa and globally, reinforcing the urgent need for preventative strategies like lifestyle audits.

Cost per incident is high

Employee fraud remains one of the most pervasive and costly risks facing organisations across Southern Africa. According to Christo Snyman, CEO of CS Forensics, investigations into over 400 employee fraud cases in the region reveal that the average financial loss per incident exceeds R2 million. These cases often go undetected for months due to misplaced internal trust, weak internal controls, and, in many instances, collusion among employees (BusinessTech, 2024).

Globally, occupational fraud is equally alarming. The Association of Certified Fraud Examiners (ACFE) estimates that businesses lose approximately 5% of their annual revenue to occupational fraud, with the vast majority of cases involving employees who exploit their legitimate access to systems and resources.



Employees are a major source of economic crime

In PwC's 2020 Global Economic Crime Survey, South African organisations reported that 41% of all reported economic crimes were committed by internal employees, 36% by external actors, and 21% involved collusion between internal and external parties.

Globally, approximately 41% of organisations reported experiencing economic crime between Q1 2022 and Q4 2023, while in Africa, the incidence was slightly higher - around 46% (PwC, 2024).

Procurement fraud remains one of the most disruptive forms of economic crime globally, with over 55% of organisations identifying it as a significant concern in their respective countries (PwC, 2024). This trend reflects rising vulnerabilities in vendor selection, contract management, and payment processes - especially where internal controls are weak or bypassed.

Despite this growing threat, nearly 20% of companies reported using no data analytics at all to detect procurement fraud, and only 59% had conducted an enterprise-wide fraud risk assessment in the previous 12 months - as reported in the 2024 PwC Global Economic Crime and Fraud Survey, which covered incidents over the period 2022 to 2023 (PwC, 2024).

This makes employee fraud a more significant threat than external cybercrime or supplier fraud in many sectors, particularly financial services and government-linked entities.

Payroll and leave-related losses are substantial

Sick-leave and payroll fraud - including practices such as ghost employees and inflated leave claims - represent a significant hidden cost for South African organisations. Estimates suggest that these forms of internal fraud may account for as much as 17% of total payroll, with industry losses believed to range between R12 billion and R16 billion annually. These figures highlight the extent to which fraudulent absenteeism and unauthorised payroll manipulation can drain resources, especially in large organisations with complex payroll systems (BusinessTech, 2025; Duja Consulting, 2024).



These schemes are often difficult to detect because they typically involve collusion between employees or occur in environments with weak oversight. Without regular audits of employee entitlements and scrutiny of potential lifestyle inconsistencies, such fraud can persist for extended periods - undermining financial performance and organisational integrity.

Detection is often reactive

Whistle-blower tips remain the most effective method for detecting employee fraud, responsible for uncovering 43% of reported cases globally - significantly outperforming internal audits (15%) and management reviews (12%) as detection mechanisms⁴.

This reactive model allows for prolonged damage, making the case for integrating lifestyle audits and behavioural monitoring into HR and risk strategies.

Reputational fallout can be long-term

Employee-driven scandals not only incur direct financial losses, but also erode customer trust, investor confidence, and brand equity.

In high-profile cases like VBS and Steinhoff, employee or executive misconduct led to massive share price collapse, public inquiries, and loss of institutional credibility.

Organisations often spend millions on legal recovery, PR crisis management, and internal restructuring—costs that far exceed the original fraud amount.

Summary implication

Employee fraud is a silent but high-impact risk - often driven by financial stress, ethical vulnerability, paucity or lack of data driven information or weak internal deterrents. The figures above point to a clear gap: early detection mechanisms like continual lifestyle audits, financial screening, and behavioural oversight must be mainstreamed into HR practice, not left solely to forensic investigations after the damage is done.

⁴ Association of Certified Fraud Examiners, Occupational Fraud 2024: Report to the Nations



The current role of risk management in lifestyle audits

While the previous section outlined the scale and cost of employee fraud, it also revealed the limitations of traditional responses that often come too late. To prevent future incidents, organisations must critically assess how lifestyle audits are currently structured and implemented. This next section examines the prevailing risk management-led model, identifying key gaps that hinder its effectiveness and make the case for a more proactive, people-centred approach.

Traditional placement of fraud risk

In most South African organisations, white-collar crime risk - including employee fraud and unethical conduct - is typically housed within the risk management or internal audit functions. These departments focus on identifying, assessing, and mitigating various operational and financial risks. Their tools often include:

INTERNAL audits and control testing

WHISTLE-BLOWER hotlines

INCIDENT reporting frameworks

FORENSIC investigations (reactive in nature)

While effective in post-incident responses, this framework is largely reactive. It focuses on what has already gone wrong, often identifying fraudulent activity only after significant damage has occurred.

Limitations of risk management in employee-centric fraud detection

The risk function was not originally designed to manage personal financial behaviours or individual ethical vulnerabilities of employees. It has several structural limitations:



NO DIRECT line of sight into personal lifestyle red flags (e.g. unexplained wealth, sudden spending surges).

LIMITED authority to intervene pre-emptively unless a breach of policy has occurred.

LACK of behavioural insight, as financial stress or lifestyle inflation might not trigger alerts under traditional enterprise risk tools.

Moreover, risk management relies heavily on data-driven triggers and exception-based reporting, missing the more nuanced red flags that might indicate an employee is susceptible to, or already engaging in, misconduct.

Gaps in preventative measures

Lifestyle audits are typically conducted only for high-level executives or politically exposed individuals or areas of the organisation that are assumed to be exposed to risk, and usually only after suspicions have been raised. Routine monitoring for early warning signs among mid-level staff or operational teams remains rare, representing a missed opportunity to detect misconduct earlier and mitigate potential risks:

DETECT potential vulnerabilities (e.g. excessive debt, dependency on loans).

INTERVENE before misconduct occurs.

ESTABLISH a culture of transparency and deterrence.

There is a growing consensus that preventative controls are just as important as detection and response, especially in key roles that exercise decision making autonomy which can benefit third parties, who would pay for a specific outcome. Yet, these controls often sit outside the remit of traditional risk teams.

A growing case for human resource involvement

As ethical risk increasingly overlaps with personal wellbeing, financial literacy, and employee behaviour, the case for shifting part of the lifestyle audit responsibility to HR grows stronger.



Human resources is already mandated to manage:

RECRUITMENT and background checks

EMPLOYEE wellbeing and support programs

DISCIPLINARY processes and internal investigations

ETHICAL culture and organisational values

However, HR teams are not currently empowered or equipped to incorporate financial health screening as a legitimate part of employee lifecycle management - despite clear evidence that financial pressure is a key driver of workplace fraud.

This growing overlap between ethics, behaviour, and wellbeing highlights the need for a more integrated approach, where HR and risk management collaborate more closely, or HR assumes a more proactive role.

The limitations of the current risk management approach highlight a critical need for change. To effectively detect and prevent employee fraud, organisations must move beyond reactive investigations and adopt a more integrated, preventative model. The next section outlines why human resources are uniquely positioned to lead this shift and how lifestyle audits can be reimaged as part of a holistic employee integrity framework.



The case for HR-led lifestyle audits

Traditional approaches to managing fraud and white-collar crime typically place responsibility within risk management or compliance units. While these functions play a vital role, they are often designed to respond after the fact - engaging only when suspicious activity is flagged, or damage has occurred. In today's high-risk environment, this reactive model is no longer sufficient.

Human resources, with its ongoing involvement across the employee lifecycle, is uniquely positioned to lead a more preventative and people-centred approach. By shifting lifestyle audit responsibilities to HR, organisations can detect early warning signs, support ethical behaviour, and embed integrity into the fabric of workplace culture. This section outlines how and why HR should take the lead in building a forward-looking fraud prevention model.

Why HR is better positioned to drive lifestyle audits

HR teams interact with employees from recruitment to resignation, giving them unparalleled access to employee information, behaviour patterns, and workplace dynamics. This continuous engagement enables HR to:

DETECT early warning signs through changes in employee behaviour or performance.

INTEGRATE risk assessments into existing processes like onboarding, training, and performance reviews.

MAINTAIN confidential and trusting relationships that encourage employees to seek help before ethical breaches occur.

Unlike risk functions that are often reactive and transactional, HR's people-centred approach allows for a more holistic and preventative strategy.



Integrating lifestyle audits into the employee lifecycle

Embedding lifestyle audits at multiple points ensures that integrity monitoring is systematic and normalized rather than sporadic or punitive:

Onboarding:

Incorporate financial and integrity checks, along with transparency about lifestyle audits, as part of induction.

Performance management:

Regular discussions can include non-financial wellness and ethical behaviour indicators, allowing for early interventions.

Exit interviews:

Capture insights on any financial or ethical concerns that might have surfaced but were not formally reported, closing potential gaps.

Such integration reduces stigma around audits and positions them as part of broader employee support and risk management.

The link between financial stress and unethical behaviour

Numerous studies and practical observations confirm that personal financial distress is a significant and most frequent red flag predictor of unethical conduct and fraud:

EMPLOYEES experiencing growing debt, sudden lifestyle changes to income, or financial hardship are more vulnerable to temptation or coercion.

FINANCIAL stress can impair decision-making, increase anxiety, and reduce loyalty to the organisation.

PROACTIVELY monitoring and supporting employees' financial wellbeing reduces these risks before they escalate into fraudulent behaviour.

By identifying financial red flags early, HR can offer assistance or counsel, potentially preventing misconduct.



Creating a culture of ethical awareness and prevention

HR is central to cultivating an organisational culture where ethical behaviour is the norm:

CLEAR communication about integrity expectations and lifestyle audits fosters transparency and trust.

TRAINING and workshops on ethics and financial wellness reinforce positive behaviours.

ENCOURAGING open dialogue reduces the fear of reporting issues and supports early remediation.

Such cultural change transforms lifestyle audits from surveillance into an empowerment tool aligned with organisational values.

Supporting employee wellbeing while managing risk growing

Effective lifestyle audits balance fraud prevention with care for employee dignity and wellbeing:

CONFIDENTIALITY and respect must guide all interactions, avoiding intrusive or arbitrary checks.

OFFERING financial education, debt counselling, and mental health support addresses root causes.

POLICIES should clearly define audit scope, employee rights, and appeal processes.

By positioning lifestyle audits as part of a broader wellbeing strategy, HR reduces resistance and builds a foundation for ethical and sustainable workplace practices. This shift empowers organisations to move beyond reactive risk control toward a proactive model of people management - one that strengthens fraud prevention, supports employee wellness, and cultivates a culture of integrity. The next section



outlines how this vision can be operationalised through a structured, HR-led framework tailored to the South African context.



A human-centred framework for lifestyle audits

As outlined in the previous section, human resource professionals are uniquely positioned to lead a shift from reactive fraud investigations to proactive prevention. Proactive prevention reduces the long-term cost of compliance and loss to the organisation. However, for this transition to be effective, lifestyle audits must be embedded within a structured framework that balances ethics, legality, behavioural insight, and employee trust. This section outlines a practical, preventative model tailored to the South African context - while also evaluating how current service providers conduct lifestyle audits, and where existing practices fall short.

Pre-employment screening enhancements

A robust lifestyle audit strategy starts with smarter hiring. Pre-employment checks should assess not just qualifications and criminal records, but also financial vulnerability and ethical alignment - without infringing on privacy rights.

Financial standing checks (with consent):

Credit and affordability checks for high-risk roles (e.g. procurement, finance, IT) can help identify vulnerabilities, provided they comply with POPIA and labour laws.

Personality and behavioural assessment:

Use of psychometric tools that assess ethical tendencies, impulsivity, and risk orientation can enhance candidate profiling and inform support strategies post-hire.

During-employment monitoring

Preventative frameworks rely on continuous, trust-based monitoring that integrates ethics into everyday people management.

Continual vs random lifestyle audits:



Routine and risk-based audits for employees in sensitive roles can identify early red flags. Audits should be conducted transparently, with documented procedures and escalation paths, and do not require the consent of the employee. Random audits, by nature select only parts of the organisation and therefore are prone to exclude risk areas which are not in the selected scope. Continual data driven audits mitigate this shortcoming.

Internal and external indicators:

Combine payroll, absenteeism, and performance data with external markers (e.g., luxury asset ownership, company registrations) to detect anomalies.

Respect for privacy and dignity:

Ensure all monitoring is consent-based, fair, and transparent. Employees should be engaged early and respectfully when concerns arise—not treated with suspicion. Wellness interventions are ideal ways to achieve this objective, plus there is a noticeable improvement in financial wellbeing as a result.

Post-incident protocols and offboarding

When misconduct is suspected or confirmed, HR should lead a multidisciplinary process that ensures both procedural fairness and organisational learning.

HR-led investigations with risk and legal:

Collaborate across functions to investigate allegations, protect evidence integrity, and safeguard employee rights.

Ethical offboarding and support:

Offer counselling or referrals where misconduct is linked to personal crises. Use findings to improve controls and close policy gaps.

Shortcomings in current practices:

Reactive use:

Most audits are triggered post-incident - too late to prevent harm.



Externalised and episodic:

Providers are often brought in as consultants, with no continuity or cultural insight. Reduced ownership within the organisation is frequently observed.

Lack of behavioural insight:

Existing models rarely integrate psychological or ethical indicators.

Employee distrust:

Investigative approaches can appear punitive, undermining trust. These approaches are often very costly.

Services are often selected from a suite of options which can be limited due to budget constraints. Dynamic, continual lifestyle audits will include current legal actions and insolvency proceedings not yet available on traditional platforms.

Toward a more robust lifestyle audit framework

To address these gaps, organisations should adopt a hybrid lifestyle audit model that combines the technical strengths of external providers with the ongoing behavioural oversight and trust-building capabilities of HR.

Key element	Strategic role
HR ownership	Builds continuity, trust, and integration across the employee lifecycle
Risk-based targeting	Focuses on high-risk roles and triggers (e.g., lifestyle inflation, red flags)
Behavioural and financial integration	Links ethics, financial stress, and employee wellbeing
Transparent policies	Ensures fairness, consent, and legal compliance
Cross-functional collaboration	Leverages HR, risk, IT, and legal for oversight and escalation

With a preventative HR framework in place, the next step is to explore how it can be adapted for high-risk sectors, particularly within financial services and the public sector, where the stakes are higher, risks more complex, and consequences significantly more severe.



Corruption and the law

South Africa has a Constitutional democracy that in its founding provisions clearly sets out values that include a one person, one vote principle, which through a multi-party democracy will “...ensure accountability, responsiveness and openness”. Supported by Chapter 9 institutions such as the Public Protector, Auditor General and the South African Human Rights Commission, public administration is expected to be governed by “...democratic values and principles enshrined in the Constitution...”.

Specific mention is made to the basic values and principles of government, including a high standard of professional ethics and transparency that apply to every sphere of government, all organs of state, and public enterprise. Simply put, the State with its substantial task of redressing the past and charting a new course for the vision of a new South Africa has to use its limited resources wisely, and procurement, a tool for transformation, would be done fairly and equitably.

In support of the Constitution, several other legal frameworks were developed.

PREVENTION and Combating of Corrupt Activities Act, 2004;

PREVENTION of Organised Crime Act, 1998;

PROTECTED Disclosures Act, 2000;

FINANCIAL Intelligence Centre Act, 2001;

PROTECTION of Constitutional Democracy Against Terrorist and Related Activities Act, 2004; and

COMPETITION Act, 1998.

In addition to these national laws, business must also comply with the Companies Act and the best practices provided by the King Report on Corporate Governance (King IV) that provides guidelines on ethical leadership, corporate responsibility and accountability.



With such a comprehensive legal framework and Chapter 9 institutions to give effect to the object of these laws, by 2016, the extent of the indifference to the rule of law, under the Zuma presidency, was exposed through the State of Capture report produced by the public protector.

The Johannesburg based Gupta family, seemingly wielded undue influence over the president, in favour of their private business interests, which included the president's son, trumped the interests of the people with the appointment of cabinet ministers and boards of state-owned entities being influenced through this relationship.

Conflicts of interest are clearly envisaged in the Executive Members' Ethics Act, which applies to cabinet members, deputy ministers and members of the executive councils of provincial parliaments who must comply with the Act when discharging their official duties. Through a systematic weakening of the government, accountability was diminished, and lifestyles flourished, giving rise to a powerlessness amongst the people, described as state capture.

2018 Conviction rates in complex commercial crimes in the Specialised Commercial Crimes Unit] – 800 cases with 760 convictions – conviction rate of 95%]

The cost of this period of state capture is being funded through the economy by those that can paying more for goods and services and taxes, and those that cannot, paying through delayed service delivery.

The FATF has in no small part sharpened the resolve of government to exit the grey listing and in so doing will have to demonstrably remediate many of the issues that have given rise to state capture. The FATF notes:

“South Africa has a relatively high volume and intensity of crime, and more than half of reported crimes fall into categories that generate proceeds. The main domestic proceeds-generating predicate crimes are tax crimes, corruption and bribery, fraud, then trafficking in illicit drugs, and environmental type crimes”.

As South Africa responds to the expectations of FATF they will have to convincingly address the observation that “...cases relating to “State capture” have not



been sufficiently pursued in the past, and corruption cases referred to the NPA by the SIU have not been dealt with expeditiously.”

The lack of information pertaining to the ultimate beneficial ownership of companies and trusts is another key deliverable that will strengthen both government and private sector’s ability to understand and evidence where potential conflicts of interest may arise.

As we build a more resilient environment that will hopefully be more responsive to all levels of corruption and fraud, both as the state and private sector, we need to enable a partnership between likeminded institutions and shift away from voluntary disclosures, manual and paper-based systems of investigation to a more modern, digitally based approach.

In 2019 the IMF noted on the fight against state capture:

“Nonetheless, given the depth and breadth of state capture, sustained efforts—especially establishment of credible deterrence mechanisms—will be required to credibly combat corruption and improve governance.”

It is these credible deterrence mechanisms that this paper will focus on, as we explore the potential for lifestyle audits to complement the existing efforts of government to restore the Constitution and its Chapter 9 institutions to their rightful place in society.



Institutional collaboration

In an increasingly complex governance landscape, where fraud and unethical conduct often go undetected until the damage is done, traditional audits and compliance systems are no longer enough. To stay ahead of evolving threats, lifestyle audits and declarations of interest must be repositioned as proactive tools for fraud mitigation—anchored in real-time insights, behavioural risk monitoring, and early detection of misconduct. This shift requires a new kind of collaboration between the Auditor-General of South Africa (**AGSA**), government departments, and the private sector.

From static audits to dynamic oversight

Although the AGSA currently conducts annual audits focused on financial and performance accountability, its role in fraud prevention can—and must—expand to meet the ethical demands of the time. While the AGSA does not conduct lifestyle audits directly or in real time, it is uniquely positioned to become a strategic enabler of real-time lifestyle monitoring systems within public entities.

AGSA can embed expectations for lifestyle audits and declarations of interest into its existing audit frameworks by:

ASSESSING whether departments have effective systems in place for ongoing lifestyle risk monitoring, particularly for high-risk roles;

REVIEWING the effectiveness and accuracy of interest declarations;

HIGHLIGHTING weaknesses in governance where employee wealth, access to funds, or procurement authority is not adequately tracked or verified;

RECOMMENDING that entities integrate lifestyle red flags and risk indicators into their internal control environments.

PRIORITISING Politically Exposed Persons (PEPS)



In doing so, the AGSA does not become the direct executor of lifestyle audits—but rather a catalyst for reform, helping institutions shift from static annual checks to dynamic, data-informed governance.

Declaration of interests: From compliance exercise to behavioural safeguard

The declaration of financial interests is often treated as a bureaucratic exercise, easily bypassed or submitted without verification. However, when digitised and cross-referenced against data from SARS, CIPC, deeds registries, and procurement systems, these declarations can evolve into live integrity tools, capable of detecting discrepancies before they escalate into fraud.

To support this shift, government departments and SOEs must be encouraged—through audit expectations and legislative reform—to:

TREAT declarations as evidence of ethical intent, not mere compliance;

CONDUCT regular verification exercises;

BUILD automated systems that flag unexplained lifestyle changes or ownership patterns inconsistent with declared income.

The AGSA can monitor whether such systems exist and function effectively, using its reports to highlight gaps and drive accountability.

The role of the private sector: Intelligence, verification, and deterrence

Private-sector actors—especially credit bureaus, financial institutions, and analytics providers—can significantly strengthen the state’s ability to monitor fraud risks. Through controlled data partnerships, these organisations can offer:

BEHAVIOURAL analytics to identify financial anomalies

VERIFICATION of declared assets and interests



TOOLS for real-time red-flag alerts tied to procurement, payroll, and financial approvals.

Such collaboration ensures that lifestyle audits and declarations of interest are not static records, but dynamic fraud prevention mechanisms embedded across the ecosystem.

Enabling a preventative model through institutional integration

To operationalise lifestyle audits and declarations of interest as fraud mitigation tools, a coordinated architecture is needed—combining the oversight authority of AGSA, the compliance role of internal HR and audit teams, and the data intelligence of the private sector.

This ecosystem would:

POSITION lifestyle monitoring as a behavioural governance tool

SUPPORT early identification of fraud risks based on intention and evidence, not just outcomes

SHIFT the system from reactionary enforcement to proactive prevention

REINFORCE public confidence through transparent, verifiable oversight.

By expanding its scope to include assessments of lifestyle monitoring systems, the AGSA can lead this transition without compromising its independence or overextending its mandate. It provides the institutional legitimacy and reporting power necessary to embed lifestyle audits and declarations of interest into the mainstream of ethical public service delivery



Evaluating the current lifestyle audit and declaration of interest system

In a survey⁵ of 252 200 completed declarations of interest, it was found that 4.4% of employees correctly declared their interests. Of all the information supplied on a declaration of interest, 41% had changed within 4 months of the submission. 7.5% of employees had some form of undeclared conflict of interest while 7.3% of employees or their family members had links to suppliers.

Low detection rates and limited scope

Since compulsory lifestyle audits for Senior Management Service (**SMS**) members began in April 2021, the system remains narrow in both reach and impact. By March 2023, DPSA reported that just 7,856 senior managers were subjected to lifestyle reviews, and only 157 cases were referred for investigation—less than 2% of all reviews triggered further action. This low referral rate suggests that reviews are not effectively identifying unethical conduct or unexplained wealth, given the public perception of high levels of corruption at all levels of government.

Early-stage implementation & weak enforcement

Despite expanding from 15 to 36 national departments and from 6 to 89 provincial departments over two years, DPSA admits the process remains unevaluated in terms of preventing fraud or corruption. Findings are often kept confidential, and disciplinary follow-up lacks transparency.

Legislative gaps and privacy constraints

⁵ Corporate Insights (Pty) Ltd



Government-issued lifestyle audit guidelines are not backed by robust legislation. They often conflict with POPIA (personal information protection) and PAIA (access to information) laws, creating legal ambiguity and limiting effective enforcement. This loophole allows officials to evade scrutiny under the guise of privacy or due-process concerns.

Data limitations and weak verification capacity

Too often, lifestyle audits rely on self-declarations, without real-time cross-referencing to SARS, CIPC, procurement records, deeds registries, or transaction data. Risk officers are under-resourced, and investigations remain qualitative and ad hoc rather than systemic. A move towards digital public infrastructure will enhance the capability of the state to perform seamless lifestyle audits as the digitalisation of data bases and services become a reality.

What these gaps mean

A REFERRAL rate below 2% suggests that fraud and unexplained enrichment may be consistently missed, not caught.

LACK of independence and capacity in investigation units undermines credibility, deterrence, and consistency.

PRIVACY and legislative objections, particularly under POPIA, are often used as convenient loopholes to avoid audit scrutiny.

Recommendations: strengthening fraud prevention tools

Expand beyond SMS - widen the net:

Utilise risk-based profiles to extend lifestyle monitoring beyond senior managers. Include:

PROCUREMENT personnel,

PAYROLL officers,



OFFICIALS with PEP or tender influence.

This ensures collusion and fraud risks are covered across levels, not just at the top.

Legal reform: enshrine lifestyle audits in law:

Translate DPSA directives into legally binding legislation—similar to Unexplained Wealth Orders or illicit enrichment frameworks in UK, Kenya, and Malaysia. This resolves conflicts with POPIA/PAIA and provides clarity around investigatory authority, data access, and consequences.

Digitise declarations: real-time cross-check and red flags:

Build a unified data ecosystem that links:

DECLARATIONS of interest,

ASSET registries,

SARS and CIPC data,

PROCUREMENT and payroll systems.

Automated alerts should flag inconsistencies between declared income and observable lifestyle changes, triggering internal review without manual intervention.

Capacity-build and independently verify:

Train risk officers and ethics committees in forensic and data analysis skills. Establish partnerships with the Special Investigation Unit (**SIU**) and the State Security Agency (SSA) to verify flagged cases and escalate them as needed, ensuring audit integrity and actionability.

Transparency, reporting, and accountability:

Standardise disclosure of aggregate results, including the number of audits conducted, investigations launched, issues resolved, and sanctions applied. A published annual report, accessible to Parliament and the public, would strengthen public confidence and increase pressure on entities to take action.



These reforms create the infrastructure needed for real-time lifestyle audit systems, which the AGSA can then review as part of its annual performance and financial audits.

It enables AGSA to assess whether departments are applying preventative integrity tools earlier in the governance cycle, without requiring AGSA to become an investigative body itself.

Challenge Area	Evidence & Impact	Recommended Fix
Narrow SMS scope	<2% referral rate from lifestyle reviews	Expand to procurement, payroll, high-risk roles
Concept lacks legal authority	Directive conflicts with POPIA/PAIA	Legislate lifestyle audits and asset declaration
Self-reporting, manual process	Risk officers lack verification data	Use linked data systems to automate red flags
Low transparency	Minimal reporting and enforcement detail	Publish annual audit outcomes, performance metrics

By addressing these gaps, especially in data, legislation, and capacity, South Africa can turn lifestyle audits and declarations into real-time, evidence-based tools for detecting fraud. This elevates audits from symbolic exercises to strategic instruments of institutional integrity and public trust.



SA lifestyle audit and fraud prevention: gaps and global benchmarks

While South Africa has taken meaningful steps to promote ethical conduct through lifestyle audits and declaration of interest systems, these measures remain fragmented, reactive, and underutilised. Globally, several countries have moved toward integrated, real-time fraud prevention frameworks that embed ethical oversight into institutional processes. This chapter benchmarks South Africa's current approach against international good practice and highlights the strategic gaps that must be addressed to enhance public and private sector fraud mitigation systems.

Preventative versus reactive approaches

Internationally, lifestyle audits are increasingly implemented as proactive mechanisms that help identify ethical risks before misconduct occurs. In countries such as Singapore, Canada, and the United Kingdom, lifestyle monitoring is embedded in human resources and compliance systems and supported by real-time data analytics.

In South Africa, the prevailing approach is reactive. Lifestyle audits are typically triggered by suspicion or reputational risk and tend to focus on senior executives or politically exposed persons. Broader application across operational teams is rare, and the use of audits as an early-warning tool remains limited.

Declarations: from annual submissions to continuous monitoring

Globally, declarations of interest are filed digitally and verified against tax, procurement, and asset registries. In Estonia, for example, public officials are required to disclose assets in real time through an accessible online system. Georgia enforces strict asset verification through civil service law, while Chile operates an open disclosure platform that feeds directly into regulatory oversight.



South Africa still relies heavily on static forms, often submitted annually in manual format. These declarations are rarely audited, with limited mechanisms to cross-check accuracy or penalise false or non-disclosure.

Oversight bodies and institutional coordination

Strong international models feature dedicated oversight agencies with clear mandates to enforce lifestyle and ethics compliance. Hong Kong's Independent Commission Against Corruption (ICAC) is a leading example, conducting investigations, public education, and systems audits under a unified structure.

In contrast, South Africa's oversight landscape is fragmented. Institutions such as the Auditor-General of South Africa (AGSA), Public Service Commission (PSC), SIU, and individual departments have overlapping responsibilities. This lack of coordination reduces the effectiveness of monitoring and enforcement.

Data sharing and real-time integration

Countries that lead in fraud detection have achieved high levels of data integration across tax authorities, land registries, procurement databases, and banking systems. Singapore and the United Kingdom have made significant progress in linking financial data with public sector oversight systems to detect lifestyle anomalies.

In South Africa, this level of interoperability does not yet exist. Privacy and information protection concerns, particularly under POPIA, are often cited as reasons for refusing data access, even when such data is critical for fraud prevention. The interpretation and implementation of POPIA have, in many cases, become barriers rather than enablers of oversight.

Private sector accountability and reporting standards

In jurisdictions such as the European Union and the United States, financial institutions are required to report incidents of internal fraud to regulators. The European Whistleblower Directive, for example, obliges private companies to



implement secure internal reporting channels and publish regular disclosures on fraud risk.

South Africa lacks a similar framework. No industry-wide standard exists for the reporting of employee fraud in banks or other high-risk sectors. Cases typically become public only through criminal prosecution or media exposure. As a result, there is little sector-level visibility into internal fraud risk or systemic vulnerabilities.

Strategic gaps in the south African system

The benchmarking exercise reveals the following five key gaps:

Area	Gap Identified
Proactive intent	Lifestyle audits are mostly forensic in nature, rather than embedded as routine risk detection tools.
Technology and data integration	Declaration systems are not linked to procurement or asset registries in real time.
Oversight fragmentation	Multiple agencies operate in silos, with overlapping roles and limited coordination.
Private sector underreporting	No centralised mechanism for reporting internal fraud incidents, especially in the banking sector.
Interpretation of privacy legislation	POPIA is often used to resist data access, even when oversight would be legally and ethically justified.

Lessons from international models

Country	Key Innovation
Singapore	Integrated monitoring using linked databases and proactive oversight mechanisms.
Estonia	Fully digitised asset declarations accessible to the public and linked to enforcement.
Georgia	Civil service laws link asset disclosure to integrity monitoring and disciplinary processes.



United Kingdom	Partnerships between tax authorities and public oversight bodies to detect unexplained wealth.
Chile	Transparent, online interest declaration platforms linked to regulatory frameworks.

The banking industry has developed a mechanism to record and share the details of dishonest employees that have been found guilty through a disciplinary process. It is therefore possible for available information to be consolidated more effectively rather than the current approach, which remains fragmented, scattered across media reports, isolated employer disclosures, and individual legal cases.

Employees will move between the public and private sectors, demonstrating that a holistic approach needs to be developed and collaboration is important. Industries or sectors that could benefit from a register of dishonest employees could include regulated industries such as financial services, telecommunications or insurance with many other organisations which work on trust, such as professional bodies, where their employees must look after the interest of the business as well as their customers.

These sources are reactive rather than proactive, incident-based instead of statistical, and do not offer trend-level insights. Within the legal rights afforded to individuals, sharing of information between employers would be useful and prevent unnecessary risk with onboarding new employees.

Additionally, while international databases like ORX track operational risk loss events, they do not clearly distinguish between fraud committed by internal employees and that perpetrated by external actors. This lack of granularity makes it challenging to analyse insider threats effectively.

The absence of a unified reporting framework limits the sector's ability to benchmark risk, identify systemic weaknesses, or develop informed prevention strategies. It also hampers public transparency and inhibits collective learning across institutions.

Strategic recommendation: a new reporting standard



To address these gaps, South Africa should consider introducing a standardised framework for reporting internal fraud within financial institutions and high-risk sectors. This new reporting standard could include:

CLEAR definitions and categories of occupational and collusive fraud.

MINIMUM thresholds and timeframes for mandatory disclosure.

AUDIT trails and procedures for flagging and escalating internal misconduct.

INTEGRATION with lifestyle audit platforms and interest declaration systems.

SECTOR-WIDE benchmarks to enable aggregated trend analysis and comparative risk reporting.

This initiative would have to be driven by the State as the legal framework would need to complement the approach to make it effective.



Conclusion

South Africa faces a persistent and costly challenge in addressing white collar crime. The evidence presented in this report—including case studies, cost analysis, system reviews, and international benchmarking—underscores a critical weakness: lifestyle audits, as currently implemented, are too reactive, too limited in scope, and too disconnected from the everyday realities of the workforce.

This report proposes a strategic and cultural shift: repositioning lifestyle audits as a proactive and preventative function embedded within human resources. Unlike risk and compliance teams, which often intervene only after wrongdoing occurs, HR is uniquely placed to detect behavioural red flags early, support ethical conduct, and build a workplace culture of transparency, trust, and accountability.

Key takeaways include:

TRADITIONAL forensic led lifestyle audits are often triggered too late, after fraud has already occurred.

HR LED audits offer continuous monitoring and behavioural insights across the employee lifecycle, enhancing early detection and employee support.

CURRENT practices suffer from legal ambiguity, lack of real time data integration, and poor coordination across institutions.

GLOBAL best practices highlight the value of digitised declarations, central oversight bodies, and data sharing frameworks, all largely missing in the South African context.

To move forward, organisations and public institutions must:

LEGISLATE lifestyle audits to strengthen enforcement and address legal grey areas such as POPIA constraints.

DIGITISE and integrate systems for declarations, asset registries, procurement, and tax data to enable automated red flag detection.



TRAIN HR teams to implement audits with empathy, confidentiality, and ethical sensitivity.

FOSTER interdepartmental collaboration, particularly between HR, risk, legal, and IT, to build cohesive prevention frameworks.

ENCOURAGE external partnerships with analytics providers to supplement internal capabilities without compromising trust.

In parallel, it is essential to address the lack of consolidated data on employee fraud. At present, fraud cases typically come to light through media coverage, internal dismissals, or criminal prosecutions. These disclosures are isolated, incident based, and not publicly tracked or analysed in an aggregated format. Key industry and regulatory bodies should be encouraged to publish regular trend analysis or sector wide reporting on occupational fraud. Collaboration can strengthen both organisational learning and the ability to benchmark risk or develop sector specific prevention strategies.

Ultimately, this is not merely a technical upgrade but a cultural transformation. It calls for a shift from treating lifestyle audits as punitive tools to recognising them as instruments of ethical leadership and institutional resilience.

South African organisations that make this shift will not only be better equipped to detect and prevent fraud, they will also contribute to rebuilding public confidence, advancing good governance, and creating workplaces where integrity is the norm, not the exception.



Bibliography

- A&O Shearman. (2024). *State capture, FATF grey-listing and cross-border white-collar crime in South Africa*. Retrieved from <https://www.aoshearman.com/en/insights/cross-border-white-collar-crime-and-investigations-review-2024/state-capture-cross-border-white-collar-crime-and-investigations-in-south-africa>
- AP. (2024). *South Africa is investigating alleged \$7B corruption at state-owned companies*. Retrieved from <https://apnews.com/article/south-africa-corruption-graft-investigations-6efc1cab8446c882758943382d6bdd3b>
- Association of Certified Fraud Examiners (ACFE). (2022). *Report to the Nations: Global Study on Occupational Fraud and Abuse*. Retrieved from: <https://www.acfe.com/report-to-the-nations/2022>
- Association of Certified Fraud Examiners. (2024). *Occupational Fraud 2024: Report to the Nations*. Available at: <https://legacy.acfe.com/report-to-the-nations/2024/>
- BBC News. (2022). *South Africa's Zondo commission: Damning report exposes rampant corruption*. Retrieved from <https://www.bbc.com/news/world-africa-61912737>
- BDO South Africa. (n.d.). *Lifestyle Audits*. Retrieved from <https://www.bdo.co.za/en-za/services/advisory/forensics/lifestyle-audits>
- BusinessTech. (2018). *The 10 most common crimes in South Africa*. Retrieved from <https://businesstech.co.za/news/lifestyle/271455/the-10-most-common-crimes-in-south-africa-and-where-theyre-most-likely-to-happen/>
- BusinessTech. (2023). *Employees are scamming their bosses in South Africa – costing them billions*. Retrieved from <https://businesstech.co.za/news/business/731767/employees-are-scamming-their-bosses-in-south-africa-costing-them-billions/>
- BusinessTech. (2024). *Employees are scamming their bosses in South Africa – costing them billions*. Retrieved from: <https://businesstech.co.za/news/business/731767/employees-are-scamming-their-bosses-in-south-africa-costing-them-billions>
- BusinessTech. (2025). *Employees are scamming their bosses in South Africa – costing them billions*. Retrieved from: <https://businesstech.co.za/news/business/731767/employees-are-scamming-their-bosses-in-south-africa-costing-them-billions>
- Chambers and Partners. (2024). *White-Collar Crime 2024 – South Africa*. Retrieved from <https://practiceguides.chambers.com/practice-guides/white-collar-crime-2024/south-africa>



Commonwealth Lawyers Association. (2025). *Declaration of assets and lifestyle audits – invaluable tools in the fight against corruption*, by Musa Mwenye SC. Retrieved from <https://www.commonwealthlawyers.com/cla/declaration-of-assets-and-lifestyle-audits-invaluable-tools-in-the-fight-against-corruption-by-musa-mwenye-sc/>

Daily Maverick. (2024). *IEC Commissioner Dr Nomsa Masuku arrested for R1.2m fraud, granted bail*. Retrieved from: <https://www.dailymaverick.co.za/article/2024-06-21-iec-commissioner-dr-nomsa-masuku-arrested-for-r1-2m-fraud-granted-bail/>

Duja Consulting. (2024). *The high price of fraud, theft, and non-compliance for South African SMEs*. Retrieved from: <https://www.duja.co.za/the-high-price-of-fraud-theft-and-non-compliance-for-south-african-smes>

Duja Consulting. (2025). *The hidden costs of ignoring lifestyle audits*. Retrieved from <https://www.linkedin.com/pulse/hidden-costs-ignoring-lifestyle-audits-duja-consulting-cvh9f/>

EthicsSA. (2023). *Ethical Leadership Handbook*. Retrieved from <https://www.tei.org.za>

Financial Times. (2023). *McKinsey pays \$122mn to resolve probes into South Africa bribes*. Retrieved from <https://www.ft.com/content/98dbb5af-1ca0-4507-abd3-11f1e69d0c62>

Institute of Risk Management South Africa (IRMSA). (2023). *Risk Report: South Africa 2023*. Retrieved from <https://www.irmsa.org.za>

IOL. (2024). *Former Absa bank employees sentenced to 15 years for R1 million fraud*. Retrieved from: <https://iol.co.za/news/crime-and-courts/2024-07-02-former-absa-bank-employees-sentenced-for-15-years-for-r1-million-fraud/>

IOL. (2024). *Former Standard Bank team leader sentenced for stealing over R3 million from client accounts*. Retrieved from: <https://iol.co.za/news/crime-and-courts/2024-08-06-former-standard-bank-team-leader-sentenced-for-stealing-over-r3-million-from-client-accounts/>

Lifestyle Audit Trends. (n.d.). *Successes, challenges & insights*. Retrieved from <https://www.duja.co.za/lifestyle-audit-trends-successes-challenges-insights/>

National Treasury. (2022). *Public Sector Anti-Corruption Strategy*. Retrieved from <https://www.treasury.gov.za>

Prospen Africa. (n.d.). *Conducting Effective Lifestyle Audits*. Retrieved from <https://prospen.co.za/conducting-effective-lifestyle-audits/>

PwC. (2024). *Global Economic Crime and Fraud Survey 2024*. Retrieved from <https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html>

PwC. (2024). *Global Economic Crime and Fraud Survey 2024: UK Perspective*. Retrieved from: <https://www.pwc.co.uk/forensic-services/assets/global-economic-crime-survey-2024-uk-perspective.pdf>



- PwC South Africa. (2022). *Economic crime and fraud survey*. Retrieved from <https://www.pwc.co.za/en/publications/economic-crime-survey.html>
- SABC News. (2019). 'PWC lifestyle audit didn't pick up 2m VBS loan to Matjila'. Retrieved from <https://www.sabcnews.com/sabcnews/pwc-lifestyle-audit-didnt-pick-up-2m-vbs-loan-to-matjila/>
- SABPP. (2023). *Code of Good Practice: Ethics in Human Resource Management*. [Incomplete link]
- SALGA. (2021). *Good Practice Guide on Municipal Financial Management*. Retrieved from <https://www.salga.org.za/Documents/Knowledge-products-per-theme/Municipal%20Finance/Good%20Practice%20Guide%20on%20Municipal%20Financial%20Management.pdf>
- South African Banking Risk Information Centre (SABRIC). (2023). *Annual Crime Statistics Report*. Retrieved from <https://www.sabric.co.za>
- South African Reserve Bank (SARB). (2023). *Financial Stability Review*. Retrieved from <https://www.resbank.co.za>
- Sutherland, E.H. (1983). *White Collar Crime: The Uncut Version*. Yale University Press.
- The DPSA. (2022). *Guide on the Prevention and Management of Conflict of Interest in the Public Sector*. [Local file – not accessible]
- The Ethics Institute. (2022). *Public Sector Ethics Survey: Ethics Risk Survey Results*. Retrieved from <https://www.tei.org.za>
- The Ethics Institute. (2025). *Public Sector Ethics Survey: Ethics Survey of National, Provincial, and Local Government*. [No link provided]
- The National Treasury. (2024). *National Treasury Update on VBS Mutual Bank*. Retrieved from: https://www.treasury.gov.za/comm_media/press/2024/2024071501%20Media%20Statement%20-%20National%20Treasury%20update%20on%20VBS%20Mutual%20Bank.pdf
- The Presidency of South Africa. (2025, July). *Progress Report on Implementation of Actions in the President's Response to the Recommendations of the State Capture Commission*. Retrieved from <https://www.thepresidency.gov.za/sites/default/files/2025-07/PROGRESS%20REPORT%20ON%20IMPLEMENTATION%20OF%20ACTIONS%20IN%20THE%20PRESIDENT%E2%80%99S%20RESPONSE%20TO%20THE%20RECOMMENDATIONS%20OF%20THE%20STATE%20CAPTURE%20COMMISSION.pdf>
- TransUnion South Africa. (n.d.). *Corporate Insights Lifestyle Assessment*. Retrieved from <https://www.transunion.co.za/product/corporate-insights>
- Uphanded Forensics. (n.d.). *Lifestyle audits and forensic & HR services*. Retrieved from <https://uphando.co.za/>



World Bank. (2020). *Guide to Preventing and Managing Conflict of Interest in the Public Sector: Good Practices Guide*. Retrieved from <https://documents1.worldbank.org/curated/en/950091599837673013/pdf/Preventing-and-Managing-Conflicts-of-Interest-in-the-Public-Sector-Good-Practices-Guide.pdf>

World Bank. (2023). *Safety First: The Economic Cost of Crime in South Africa*. Retrieved from <https://documents1.worldbank.org/curated/en/099111723083017868/pdf/P180139079ce0406a09305024e058b594e2.pdf>

Zondo Commission Reports. (2022). Retrieved from: <https://www.statecapture.org.za>

