WERKSMANS
ATTORNEYS



BUSINESS CRIMES & INVESTIGATIONS

Safeguarding business integrity

18 November 2026 *5 min read*

by Bernard Hotz, Director and Head of Business Crimes & Investigations

Economic crime presents financial, operational and reputational risks for South African businesses. As perpetrators adopt increasingly sophisticated methods, organisations must regularly assess whether their controls remain appropriate to the risks they face.

International Fraud Awareness Week, observed from 15 to 21 November 2026, offers businesses an opportunity to review their approach to preventing, detecting and responding to fraud. Awareness and education are important, but their effectiveness depends on the legal frameworks, internal controls and accountability mechanisms that support them. For boards and executives, this requires an understanding of both the organisation's exposure to economic crime and the legal obligations that arise when suspected wrongdoing comes to light.

Weak procurement oversight, inadequate segregation of duties and insufficient scrutiny of third-party relationships can create opportunities for economic crime. These risks increase where approval processes are routinely bypassed or employees are uncertain about how to report concerns.

An effective compliance framework should translate an organisation's ethical commitments into clear responsibilities, practical procedures and consistent oversight. Policies should reflect how the business operates, identify areas of heightened exposure and establish how suspected misconduct will be escalated and investigated.

Practical measures to support this include:

- Screening employees at every level: Conduct appropriate background checks on new employees, including senior and highly qualified appointments.
- Verifying suppliers: Check supplier identities, addresses and banking details before approving them, and scrutinise changes to those details.
- Using technology to identify warning signs: Use monitoring tools to flag duplicate invoices, unusual transactions and potential undisclosed relationships between employees and suppliers, including family connections.
- Strengthening IT security: Maintain appropriate safeguards to reduce the risk of unauthorised access to company systems and data.

Regular assessments can help determine whether these measures work in practice. A policy may be comprehensive on paper but offer limited protection if employees do not understand it or management fails to enforce it.

South Africa's anti-corruption legislation gives businesses a further reason to examine the gap between policy and practice. Section 34A of the Prevention and Combating of Corrupt Activities Act 12 of 2004 (PRECCA) creates an offence for a private-sector business or incorporated state-owned entity where an associated person gives, agrees or offers to give gratification prohibited under Chapter 2, intending to obtain or retain business or an advantage in the conduct of business for it. An associated person is someone performing services for or on its behalf, potentially including employees, agents, contractors and consultants.

No offence is committed under this provision where the business or entity had adequate procedures in place designed to prevent that conduct. Businesses should therefore assess whether their anti-corruption measures address how they actually operate, including the intermediaries they use and the transactions that present the greatest risk.

When suspected fraud is uncovered, the immediate commercial instinct may be to limit disruption. A resignation, confidential settlement or internal disciplinary process does not discharge an applicable statutory reporting duty. Failure to comply is itself an offence.

Section 34 of PRECCA places reporting duties on persons holding defined positions of authority, including company directors, managers and company secretaries. It covers specified corruption offences and offences including theft, fraud, extortion, forgery and uttering a forged document involving R100,000 or more.

The obligation extends beyond actual knowledge to circumstances in which the person ought reasonably to have known or suspected that an offence had been committed. Businesses should therefore avoid assuming that they can wait for a completed internal investigation before considering whether reporting is required. Reports under this provision must be made to a police official in the Hawks.

The consequences of failing to report can be substantial. PRECCA provides for a fine or imprisonment of up to 10 years where sentence is imposed by a High Court or regional court.

Directors cannot eliminate every opportunity for fraud. They can, however, require meaningful information about the risks facing the business, whether controls are working and how concerns are being addressed.

Section 76 of the Companies Act 71 of 2008 requires directors to act in good faith, for a proper purpose and in the company's best interests. They must also exercise the care, skill and diligence reasonably expected, taking account of their functions and their own knowledge and experience.

Where failures of oversight amount to a breach of these duties and cause loss to the company, personal liability may arise under section 77. Liability depends on the applicable legal requirements and circumstances; the occurrence of fraud does not, by itself, establish a director's liability.

The King V Report on Corporate Governance further supports ethical and effective leadership, with principles addressing ethics, risk, compliance and assurance. King V supersedes King IV for financial years beginning on or after 1 January 2026. Its recommended practices should be applied with regard to the organisation's circumstances, rather than treated as inflexible statutory rules.

Boards and executives should use International Fraud Awareness Week to assess whether their organisations are equipped to prevent economic crime and respond appropriately when concerns arise.

Key priorities include:

- Reviewing risk and controls: Assess procurement, payment and third-party processes, including whether anti-corruption procedures remain appropriate as the business changes.
- Clarifying reporting responsibilities: Ensure that persons in positions of authority understand when statutory reporting duties arise and how to comply.
- Testing whistleblowing arrangements: Assess whether reporting channels are accessible, confidentiality is appropriately managed and safeguards against retaliation operate effectively.
- Preparing for investigations: Ensure that investigators have the skills and technology appropriate to the suspected misconduct, preserve documents and electronic evidence, and establish how specialist expertise will be obtained where required.
- Following through on findings: Consider appropriate disciplinary action, civil recovery and criminal reporting, and address the control weaknesses identified.

Safeguarding business integrity requires sustained attention across prevention, detection, investigation and legal action where necessary. A framework that is regularly tested and consistently applied places an organisation in a stronger position to identify wrongdoing, meet its obligations and pursue recovery when losses occur.



Bernard Hotz

Head of Business Crimes & Investigations

View Profile