HOW EXPOSED IS YOUR BUSINESS TO COMMERCIAL CRIME?

The Minimum Requirements from a Commercial Crime Prevention Perspective

March 2022 Newsletter

16th Edition

RMG

Table of Contents

Introduction 3

Defining Commercial Crime 3

Importance of adopting a commercial crime risk prevention strategy 5

Effects of the absence of a commercial crime risk prevention strategy 6

Operational Business pillars 7

- Governance 7
- Human Resources 7
- Procurement 8
- Finance 9
- Information Technology 9

Bibliography 10

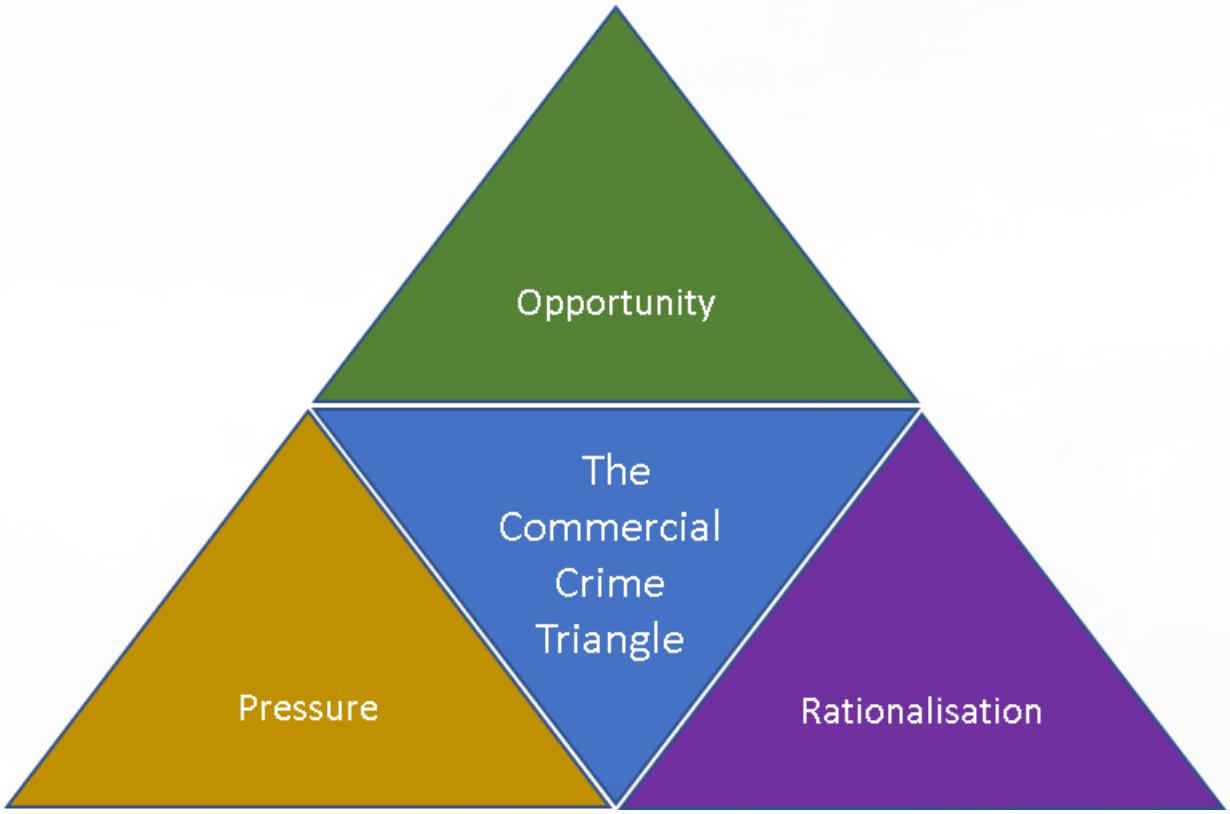
Introduction

Fraud and corruption are phrases that have become widespread in South Africa, used colloquially by individuals from all walks of life. Fraud and corruption are considered subtypes of Commercial Crime, an umbrella term that refers to all monetary criminal activities that occur within the workplace and against an organisation. The surge of commercial crime poses a risk to organisations, knowing about commercial crime is not enough – organisations are required to maintain and manage their commercial crime risks as prevention is better than after-the fact response. If a commercial crime is prevented, all the subsequent cost and time to resolve the commercial crime incident is saved. Commercial Crime Prevention Standards help to reduce visible opportunities for commercial crime occurring.

Defining Commercial Crime

White-collar crime, a term most individuals are familiar with, has ordinarily been associated with criminal activities that occur within a corporate environment. Bearing the concept of white-collar crime in mind, we broaden the delineation of commercial crime to include all monetary criminal activities that occur within the workplace as well as against organisations. Commercial crime refers to crimes committed for financial gain and includes, but is not limited to, fraud, theft, forgery, corruption, tax evasion, and money laundering in the South African context. Commercial crime is extended to include the facilitation, receiving, and possessing of proceeds from these illicit activities. Commercial crime is more easily concealed when compared to other types of crime as commercial crime entails goods or services that are inherently legal. Commercial crime is non-violent, financially motivated and generates an unmerited income. The term “commercial crime” is used here as an all-encompassing term to convey economic crime in all forms perpetrated within a business environment. One should be cognisant of the fact that commercial crime can stem from both inside an organisation, as well as outside. Internal commercial crime could be committed by employees of an organisation, while external commercial crime could be perpetrated by individuals outside of the confines of the company or entity.

Understanding the motivation behind commercial crime is the first step to maintaining your commercial crime risk exposure – you cannot manage your risk exposure without understanding where it stems from. Commercial crime arises when three conditions are present namely, perceived opportunity; opportunity; and rationalisation. The three factors are collectively referred to as The Commercial Crime Triangle, depicted below:



The Commercial Crime Triangle

Opportunity is how the commercial crime is committed. Some examples may include poor internal controls utilised by the organisation; a history of treating commercial crimes with leniency; low commercial crime awareness amongst employees; and rapid turnover of employees.

Pressure is how the commercial crime is committed. Some examples may include poor internal controls utilised by the organisation; a history of treating commercial crimes with leniency; low commercial crime awareness amongst employees; and rapid turnover of employees.

Importance of adopting a commercial crime risk prevention strategy

Without any tall tales, we acknowledge that developing and maintaining a commercial crime risk prevention strategy can be an intensive exercise. Implementing an effective strategy has many benefits and, as the saying goes, *what you sew, you will reap*. The Commercial Crime Standards were identified and developed to simplify the process of commercial crime risk management and enable effective control thereof. An efficient strategy has far-reaching implications, such as:

- Build a company culture that promotes ethical decision-making and law-abiding conduct throughout its human capital and service providers.
- Develop strategies aimed at addressing ways in which the organisation engages with and responds to commercial crime or the risk thereof.
- Identify the root causes of commercial crime both within your industry and within your organisation.
- Importantly, it will enhance the quality of the organisation's workforce.
- Reduce the risk of employees perpetrating commercial crimes against the organisation.
- Securing the organisation's assets, minimising the liabilities and protecting the cash flow of the organisation.
- Secure a safer transactional environment which will promote sustainable economic development.
- Demonstrate resilience within the organisation, which is the capacity to recover quickly and effectively from adversities.
- Limit commercial crime risk exposure posed to insurers, underwriters and investors.

Effects of the absence of a commercial crime risk prevention strategy

Organisations who successfully maintain their commercial crime risk are rewarded in a multitude of ways, such as saving with cheaper business insurance premiums, benefiting from an exceptional public perception, and retaining highly integrable employees. On the other hand, the absence of a commercial crime risk prevention strategy opens a can of worms for any organisation. It goes without saying that the biggest risk of having a poorly structured commercial crime risk prevention strategy is that it exposes the organisation to potential commercial crime which in turn results in financial loss and reputational risk. Poor internal controls enable employees to perpetrate commercial crime from within the organisation, and the lack of standard procedures and policies enable outsiders to commit commercial crime targeting the organisation.

Secondary effects may include an increase in insurance premiums; negative public opinion on the company; indirectly reduces the quality of economic growth; hinders a quality company culture; decrease in stock prices; and loss in shareholder confidence, amongst others. It will furthermore undermine the importance of the correct ethical collective approach, and increase the costs associated with formal criminal justice system procedures. The risk of harmful effects occurring will intensify and have a negative effect on the organisation itself along with the individuals within it.

Below is an example of reputational risk after the fact:

Suspect arrested for R1 million worth of fraud and theft

2021/04/13

Media Statement
Directorate for Priority Crime Investigation (HAWKS)

GAUTENG – Hawks' Serious Commercial Crime Investigation in Johannesburg arrested a female suspect on fraud and theft allegations on Monday, 12 April.

It is alleged that the suspect, Petronella Stander (51) who was employed as an accountant at a Randburg based industrial automation software and weighbridge installation company, OPTO Africa (Pty) Ltd between 2016 and 2020, allegedly swindled approximately R1 million in numerous transactions meant for suppliers into her bank account.

The matter was referred to the Hawks' Serious Commercial Crime Investigation for further investigation. A warrant of arrest was issued for her apprehension and she handed herself in at the Johannesburg Hawks office on Monday and subsequently charged.

Stander appeared in the Randburg Magistrates Court on Tuesday and was remanded in custody. The case is postponed to 20 April 2021 for formal bail application.

Operational Business pillars

Different pillars in an organisation serve different functions, as such each pillar would have unique operational risk and would require pillar-specific internal controls. Some internal controls may be used throughout different business pillars, such as segregation of duties. Segregation of duties splits business functions into different key aspects and assigns each aspect to a different individual or department. In this way, one person would not be able to complete a business transaction without the approval or assistance of another individual. For example, sourcing consumables/ products/materials and selecting a supplier would be separate functions, whereas placing an order with a supplier, and paying the supplier's invoice would again be separate functions. Further, within the IT department, software developers should not access to operational systems.

- **Governance**

  Good corporate governance sets the tone within the organisation from top to bottom. It is imperative to set up an effective Board of Directors that is aligned with legislation and policies in the countries of operation. In such way the Board will function with integrity, serving the best interests of the organisation. The effectiveness of the Board of Directors should be evaluated on an annual basis to ensure their agendas are met. It is the duty of the Board to fomalise, communicate and implement policies, processes, and procedures. Control measures that can be deployed within top management include the Board meeting on a regular basis, having an effective internal audit function and implementing external audit. Provision is made for the outsourcing of internal audit functions; however, the internal audit function should report to an audit committee. The internal audit function's work should be risk-based and performed according to International best practices. Risk management should be performed regularly and include Strategic, Operational, Commercial Crime and Information Technology areas.

- **Human Resources**

  The human resources area is commonly associated with the occurrence of commercial crime. Preventative internal controls may include ensuring work

time is documented and overtime is approved and monitored, the disciplinary and grievance process has been formalised, there is a management system within HR to monitor and manage the department, role and job descriptions for employees, rotation of staff in high-risk areas, and regularly updated policies and procedures. The Code of Ethics, policies and procedures should be communicated to employees and their acceptance documented, such as by signing the documents and proper record keeping and providing employee handbooks. Adequate screening of potential employees should be conducted to maintain the integrity of the organisation's human capital, such as by conducting criminal and background verifications and reference confirmation. Screening of employees should be conducted through an effective and formalised hiring process. An orientation programme is an important tool to educate and train new employees on the policies and procedures, and workplace rules of the company. It is becoming more common to outsource human resources functions, and it is advised that formal agreements should be in place to manage outsourced services. To prevent the occurrence of ghost employees, physical head counts should be conducted on a regular basis and compared to actual payroll. The performance of employees should be based on the competency levels for specific positions and linked to the job descriptions for the position. Further to a formalised grievance process, a whistleblower's policy should be in place to allow for employees or outsiders to anonymously and confidently report actual or suspected acts of commercial crime.

- **Procurement**

Procurement deals with the acquisition of goods or services from outside the organisation, an obvious high-risk area within business. The procurement process should be formalised and communicated to employees within the procurement space. Further, the process of making decisions should be well-documented and transparent. It is advised to have formal and well-written agreements with suppliers of good and services. Preventative internal controls may include ensuring effective policies and procedures, conflicts of interest are declared and adjudicated, proper due diligence and verification of suppliers,

and that the performance of suppliers is monitored and measured constantly. Lastly, if BEE is a requirement it should be considered and applied.

- **Finance**

The handling of hard cash and monetary equivalents needs to be cautiously controlled internally with well-documented policies and procedures. To prevent the commercial crime risk organisations should implement measures such as a documented Authority/Mandate matrix that indicates different levels of authorisation, regularly updating Risk Registers, physical checks of assets including stock checks, dual level of approval on transactions and banking, journals to be approved as per the Authority matrix on a monthly basis, and management accounts to be reviewed regularly. Payroll reconciliations should be done on a monthly basis. Further, monthly management accounts with variances should be produced and the difference between budget and actual should be explained and supported. Balance sheet items should be reconciled regularly, where required daily or monthly. Taxes should be recorded properly and paid over to the relevant Revenue authorities. Financial features such as sales, debtors, receipts, cash and bank, purchasing, creditors and payments, and assets and liabilities should be managed properly, and recorded completed and accurately.

- **Information Technology**

Upholding the Information Technology pillar is crucial to upholding the virtual integrity of the organisation and can be achieved by having an Information Technology Strategic and Operational Plan and formalised Information Security Policies and Procedures. Internal control measures include ensuring that audit trails and audit logs exist in critical systems, performing vulnerability testing and penetration testing on a regular basis, having a password policy in place, and ensuring the physical security of data centres and other premises. Further, only employees who should have access to information/data in terms of their job description should have that access. For optimal functioning, an organisation should align Information Security to best practices such as ISO27000 series. While it is accepted to outsource IT functions to external providers, due

diligence should be performed on the service providers. Operational security should be implemented and ensure that firewalls are in place, anti-malware software employed, monitoring of systems and backups made. Monitoring of systems should be done to ensure high performance and minimal downtime. An updated Hardware, Software and Information asset register should be in place. Lastly, information security training should be done with all employees and their acceptable of standard procedures and policies documented.

Bibliography

King Code of Governance Principles

Companies Act 71 of 2008

South African Police Services ("SAPS") Webpage