# Crime, Fraud and Criminality Risk Guide

## Contents

## What is Crime, Fraud and Criminality Risk?

Fraud, Theft, Robbery and Criminality (economic crime) are endemic to all organisations where money, assets and people are involved. Community Schemes are not exempt from this threat.

The size and scale of these can vary greatly and can extend back over a lengthy period. Criminals are always one step ahead and Office bearers need to be permanently on their guard. The impacts of crime can vary greatly, but most Community Schemes will not be able to survive or recover from a material financial loss without comprehensive insurance being in place, or a special levy being raised.

Not only is the number of incidences increasing, but the sophistication of the crimes is also on the rise as technology evolves and Office bearers and employees become increasingly implicated in criminality. Crimes range from simple basic thefts to very complex accounting frauds to ones involving organised crime syndicates which look to infiltrate specific industries.

Crime (fraud, theft, and criminality) risks are risks that are the result of criminal behaviour. Risks emanating from crime can have a material impact on the operations and financial position of a Community Scheme, as a result of a direct or indirect loss.

While crime generally manifests itself in financial losses, it can also impact many other areas, including operations and reputation (e.g. inability to operate optimally or insufficient resources to keep up maintenance).

These impacts can be immediate and significant or happen over a while but will have a lasting effect on the Community Scheme.

Fraud, theft, and criminality risk management start with a review of the potential criminal threats and assesses how vulnerable the Community Scheme is to crime. This should include a review of the level of governance – processes, procedures, controls, systems and people management and the effectiveness of crime controls throughout the Community Scheme. The incidents of crime there have

been and the extent to which owners/tenants/ lessees/ residents/ visitors or employees have been victims of crime e.g. robbery, theft, break-in, violent acts, muggings etc. in and around the Community Scheme in the recent past, should also be evaluated.

Crime experience and potential risk due to changing socio-economic circumstances may well force a Community Scheme to review/increase its security measures. This may require increased guards, better use of technology (sensors/beams), increased/improved access controls and additional use of cameras.

The management of fraud, theft and criminality risk will ensure that the Community Scheme is better equipped to identify, deter/prevent and deal with fraud, theft and criminal incidents or situations in a structured and effective way.

## Risk Management

To manage these risks, you must place a specific focus on financial controls around people and systems. You have to be extra vigilant around asset controls, particularly cash and moveable assets, the people you employ, your payroll, physical security, banking system access, payment systems, and procurement processes and undertake KYC of all the suppliers and contractors to the Community Scheme.

A Community Scheme needs a risk culture that is aligned with policies, processes, procedures, systems, and controls to manage the risk of fraud, theft and criminality effectively. The culture needs to place a high priority on financial controls and discipline, fraud awareness, tight asset controls, clear segregations/separations of duty, accurate and timeous financial reporting and one that endorses financial accountability at all levels. A lack of general financial controls, accountability and daily oversight will facilitate fraud, theft, and criminality.

People will always look for gaps or weaknesses in controls. A zero-tolerance approach needs to be reinforced in induction, employment contracts, and training and extended into formalised disciplinary processes.

Fraud, theft, and criminality are not confined to operational employees. Office Bearers are also often guilty of sophisticated accounting fraud, manipulation of financials and false or fraudulent reporting. Incentive plans linked to performance and related measures can unfortunately encourage inappropriate behavior and greed. Board oversight and other controls measures like independent external and internal audit controls might be necessary.

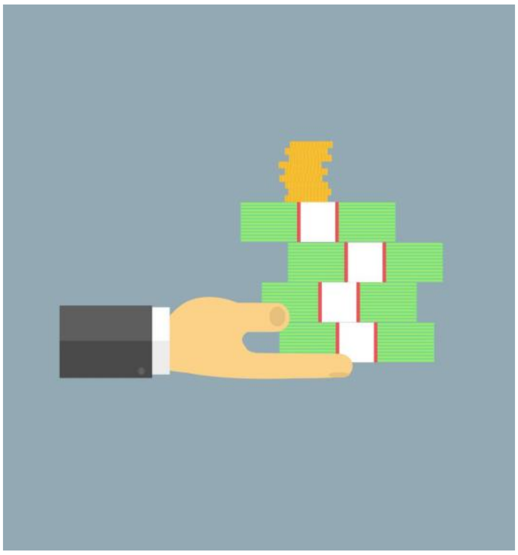
High-risk employees in the Community Scheme pose a specific risk. As such it is important that these aspects are detected before formal recruitment and engagement e.g. work references, criminal record checks, credit checks, and ID verification.

As Office bearers, you need to be aware of high-risk behaviour and lifestyle changes i.e. gambling addictions, drug addiction, high levels of debt, new vehicles, and overseas trips. Employees who have specific responsibilities and accountabilities but who loathe complying with set-down processes or having any oversight over them or the assets under their control need particular attention.

A high-risk employee will pose a great risk to a Community Scheme and is not only a risk to the Community Scheme but also to fellow workers and owners.

## Cash, Banking, Collection and Payroll Controls to Counter Fraud/Theft and Criminality

These areas are singularly the biggest contributors to fraud, theft, and loss. Cash is a core ingredient for fraud and theft in an organisation. The mere presence of cash in your Community Scheme makes it a target for not just criminals but for your employees as well, who will constantly be looking to exploit loopholes or gaps in controls.



The safety of residents, staff, visitors, and customers of Community Schemes where large amounts of cash are present, will always be under threat too.

With eCommerce growing at exponential rates, so too has the criminal focus and effort shifted. This has seen ever-increasing attempts being made to infiltrate existing business processes, collusion with and among staff, deviation from and/or circumvention of procedures and controls, and interception and/or diversion of payments and collections.

Fraud and thefts are well coordinated among syndicate participants, slick in execution and well timed. Given that this area is now the most vulnerable to attack by outsiders and employees, very strict disciplines and controls need to be deployed. A Community Scheme managing its bank accounts and payments becomes highly vulnerable to its banking applications and systems being compromised or hacked and its bank accounts and/or credit card details being compromised if tight security controls and disciplines are not deployed.

The deviation of monies via payment and/or collections using electronic transfers into third-party bank accounts is the most effective and quickest way for employees and syndicates to steal and embezzle funds. The "altering" of beneficiary bank details or the "creation" of "beneficiaries" being a common area of fraud. It is thus essential that duties, capabilities, and responsibilities around banking systems are segregated.

Procurement of consumables/stock/materials or assets such as vehicles or equipment over the web is another area that needs to be handled very carefully. Buying or purchasing items from random sellers or suppliers on the web or social media where you are required to pay a deposit or amounts into a bank account upfront, is highly risky and prone to fraud unless the beneficiary is known and credible with a known track record.

Lifestyle expenditure is one of the major reasons driving fraud. This applies to not only employees but to Office Bearers of the Community Scheme. The situation is aggravated where the socio-economic environment is adverse, or where the Community Scheme may no longer be performing well with revenues under pressure. Office Bearers or employees have lifestyle expenses that still need to be met, and the resources of the Community Scheme become easily targeted.


Conflicts of interest are another area that can give rise to corruption, losses and kickbacks. It is important that these are disclosed by Office bearers or employees in a position of influence. Conflicts can influence contractor, supplier and service provider selection, the levels of business given, orders and tenders, the extension of "credit"/delayed payment terms to individual owners, unwarranted pricing or sales terms and impact on legal recourse and the maintaining of an objective arms-length with owners, customers, contractors, service providers or suppliers.

Where the Community Scheme makes use of the services of a contracted security service provider or privately contracted/employed guards, it is important that the security service provider is registered with the appropriate authority, that it holds the necessary indemnity cover and that all their security guards are formally accredited. While it is important that the guards deployed are knowledgeable of the requirements of the Community Scheme where they are based and are knowledgeable of the tenants/occupants, suppliers and contractors, the rotation of guards does remain important.

The Community Scheme must consistently be taking proactive measures to improve its security and access controls making use of the latest technology e.g. provision of panic buttons to residents, maintenance of an accurate resident/servant database, number plate/drivers licence recording, pin approved third-party/visitor entry, fingerprint or facial recognition, use of CCTV cameras, motion sensors in sensitive areas, thermal imaging, and the use of drones in larger estates etc.

It is important that the Community Scheme knows the full details of everyone who is resident, or temporarily always based in the Community Scheme. This includes the employees/staff of contractors/service providers, visitors, and domestic servants, who have been granted approved access to the Community Scheme.

The Community Scheme/Managing Agents/Estate Management should have a crime reporting line or confidential reporting mechanism in place. A detailed record of all crime incidents within and impacting the Community Scheme should be kept, as well as copies of access records and CCTV data records of the Community Scheme.

As part of crime and criminality prevention, the Office bearers should take immediate measures to deal with high-risk tenants, suspicious lessees, or owners e.g., units rented for cash, units bought with laundered money, parties undertaking or conducting criminal activity, drug dealing or other suspicious or unacceptable behaviour from units/properties.

## Use of effective lighting for Safety and Security

Lighting is an often, overlooked security measure but as well as providing a necessary component for other security elements such as manned patrols or CCTV, it can also stand on its right providing a deterrence against intruders and reassurance to residents.
Adequate lighting in the right places is important to the safety and security of your Community Scheme, its residents, employees, and visitors. Proper lighting can also enhance the efficiency of your operations.

- Light critical areas such as entrance areas and gates, reception areas, passageways, perimeter fences, vehicle parks, communal facilities, and storage areas.
- Consider using glare lighting as a deterrent. It can blind intruders, making it difficult for them to see who or what is in their vicinity.
- Put exterior lights or spotlights on motion sensors or control them with photocells that turn them on and off according to the amount of natural light available.
  Motion sensors can detect motion through the use of passive infrared technology. Manual switches and timers are less effective.
- In addition to bringing light to shadows and increasing the visibility around your Community Scheme an outdoor lighting system can be a huge help to surveillance cameras.
- Consider placing some of your security lighting on a timer so that it turns on and off at a specified time by using smart timers.
- Back-up power and/or the use of solar power becomes an integral consideration for continuous lighting.