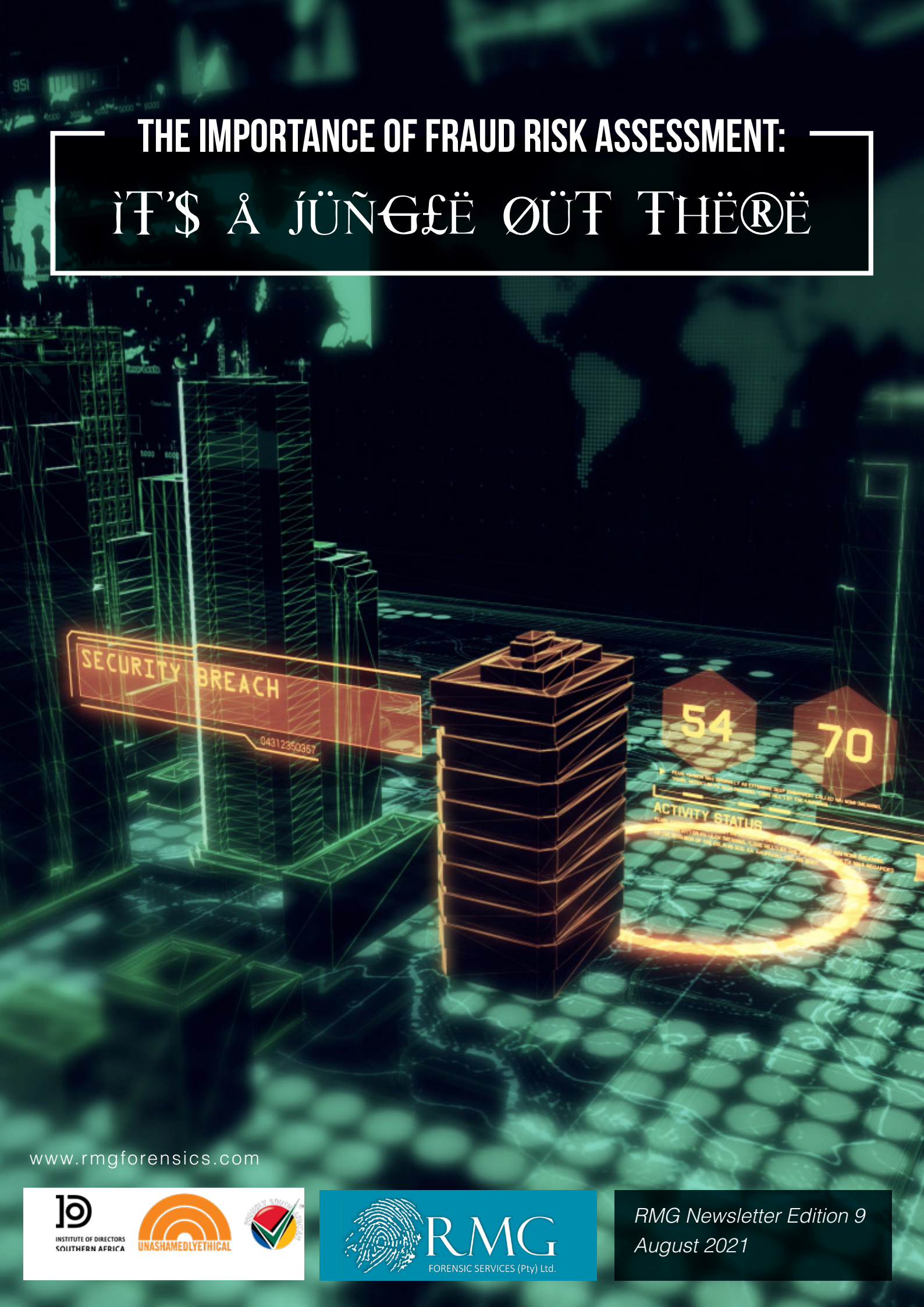
# THE IMPORTANCE OF FRAUD RISK ASSESSMENT:

## ÌF'$ Å JÜÑGŁË ØÜT ŦHË®Ë



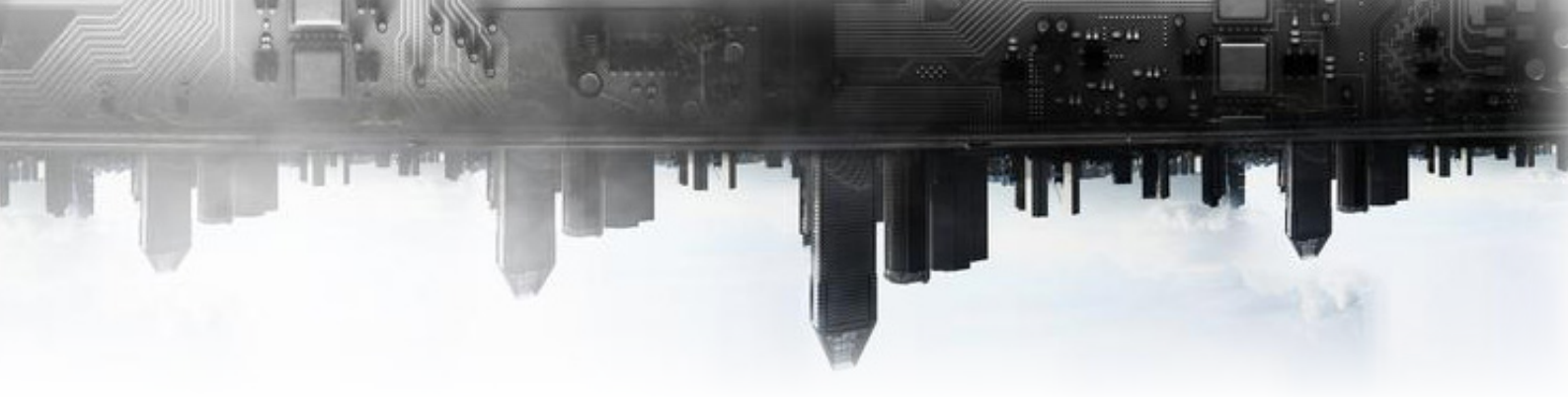

www.rmgforensics.com

INSTITUTE OF DIRECTORS SOUTHERN AFRICA

UNASHAMEDLYETHICAL

RMG FORENSIC SERVICES (Pty) Ltd.

*RMG Newsletter Edition 9*
*August 2021*



## Introduction

An organization can never exist without risk. This is an absolute that can never be changed, and it is the response to risks that define the longevity of an organization. One of the most enduring risks that an organization can face is in how much fraudulent behavior can influence its lifespan or bottom line. The institute of internal auditors defines fraud as "any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence of physical force. Frauds are perpetrated by parties and organizations to obtain money, property or services; to avoid payment or loss of services or to secure personal or business advantage".

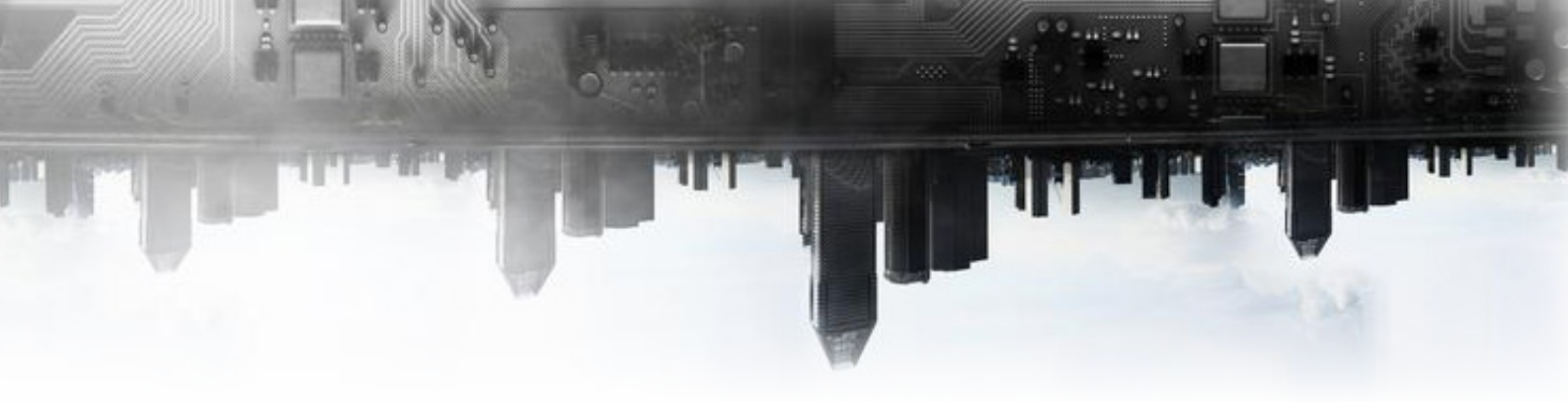
This means that fraud is something that the organization must be vigilant at all times as fraud is usually done by reason of two factors; need or greed. Although there are several defining factors that can lead to fraud within the organization it is important to note that not all fraudsters are evil hackers who are waiting for an opening, fraud can come from within the organization is an employee has reached desperation and has found no other option. And the organization can protect itself to by utilizing a fraud risk assessment within its management architecture.

Though guidelines exist on how to structure a fraud risk assessment it is advisable to have one tailor made to the organization's needs, industry, and operations that it performs. An effective fraud risk assessment should always include risk identification, assessment of inherent fraud risk and the amount of exposure the organization has towards those risks. Early detection or mitigation of fraud is key to the survival of the organization, if fraud is detected after the fraudulent act had occurred there is usually a loss to the organization. A study by the certified fraud examiners suggested that a typical organization loses approximately 7% of its annual revenue to fraud.

It is the responsibility of the organization within its structured risk planning and management that there exists a fraud risk assessment to be available to identify, resolve and react to any fraudulent activity that comes to light. The fraud risk assessment should be done at least annually but it is recommended that it is robustly reviewed regularly to identify any new or growing concerns for the organization but must be subject to change if there is a change in either internal or external factors linked with the organization.

## Techniques

As stated before, fraud is committed out of necessity or for personal gain. But within that basis exists another level that using the fraud triangle it becomes easier for the organization to identify individuals who are more likely to commit fraud. If there is an opportunity to commit fraud and enough pressure or incentive to rationalize that individual to commit fraud. The fraud risk assessment of any organization should make strong use of the fraud triangle to determine its greatest threats. The fraud risk assessment should also consider internal factors that could affect the organization such as the misappropriation of company assets or overstating expenses, overbilling customers etc. The organization must make provisions to deal with risks that come from external sources such as hacking, phishing, or reporting fraud from suppliers or customers. The fraud risk assessment may seem daunting at first, but it is a steppingstone towards a more secure and healthy business environment and culture. If the culture of fraud awareness is prevalent in the workforce, it will only strengthen the anti-fraud controls that the organization has put in place to both identify and combat fraud. Understanding this means that no one is exempt from these policies and the fraud risk assessment must address all persons affiliated within the structure of the organization. While disgruntled employees may misappropriate company assets, higher ranking employees sometimes take advantage of their position by embezzling company funds. Fraud can come from any direction, so it is advisable to have an external



audit and assessment done regularly to determine the efficacy of anti-fraud controls.

The organization has a myriad of options to assist within its tailor-made fraud risk assessment, but the interpretation of this data is as important as gathering it. Many times, fraudsters take advantage of this lack of monitoring to try and execute their insidious schemes because they have no fear of discovery. That is why having a strong key to determine the outcome of the data is as important as the assessment itself.

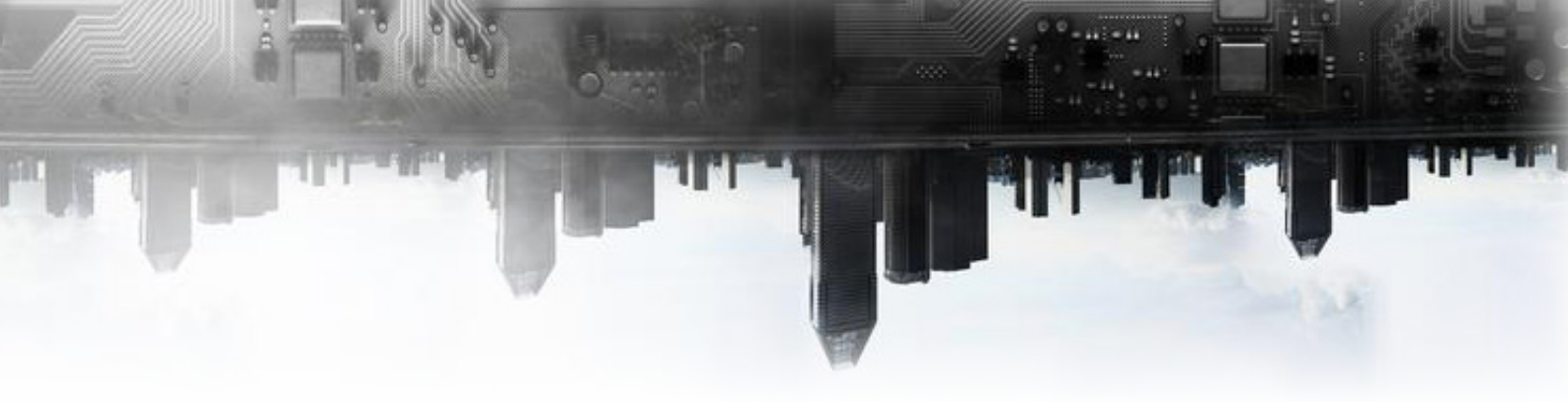
The assessment commonly makes use of surveys, interviews, and workshops to gather data to perform the fraud risk assessment. These surveys can be done confidentially in order to encourage honest answers from workers. Although useful these surveys need to be updated and reviewed regularly by management in order to ascertain its credibility. Surveys can be done on work performed, worker satisfaction as well as externally such as customer satisfaction surveys. These are all tools that can be used to gather interpretable data. Interviews and workshops are often overlooked in terms of what data can be gathered. It is important to understand how the lower rung workforce would be incentivized to commit fraud and through interaction it would be possible to speculate scenarios that can be addressed in company policy and taken into consideration when reviewing the Fraud risk assessment. When these tools are utilized correctly individuals within the company may bring attention to management fraud risks and scenarios that management had not considered, and controls can be put in place to negate and mitigate those risks.

Documentation is also an immensely powerful tool that management can use to assess fraud risk. By doing regular review and analysis of documents processed within the company there are possibilities to identify fraudulent activity (e.g., creating false documents, claiming inordinate expenses for work done). It is important to keep track of any expenses within the organization with different links in the chain or responsibility to ensure the authenticity of those logs. This is why electronic reporting is a large step for any company to ensure that their exposure to fraud risk is minimized. Electronic data is much harder to manipulate than data that contains human action to record it. Using applications and systems may influence an expenditure for the company but it is a small cost for the peace of mind that comes with business security. If there is an anomaly is found within documented data in the organization immediate action must be taken within the fraud risk assessment to address the issue and formulate controls to mitigate reoccurrences.

It is important to regularly review any data that the organization has gathered and then assess the areas and scenarios that risks are more likely to happen. Once identified the organization can implement policies and procedures to act as anti-fraud controls to minimize the exposure to the identified risks. It is also important to address within the fraud risk assessment the response that the company will have to the risk should it take place and processes in place to find the party who is responsible for allowing the fraudulent activity to occur though either gross negligence, ignorance towards the type of fraud or accidental mistakes as fraudsters tend not to care who is affected within the company by their actions.

## Open communication channels

Within the organization there must exist an anti-fraud awareness culture that management must explicitly state in their code of conduct. This will allow fraud reviews and assessments to be more honest with the information that is being supplied by the workforce. If employee moral is low it could lead to a disgruntled employee trying to exact revenge upon the company, and without an open communication channel management will have no knowledge of the feelings of the individual. These “bad apples” can spread and influence other employees if the situation is not addressed early which could lead to fraudulent activity being done within the organization



or that the workforce simply does not care to verify the authenticity of claims and information from suppliers and clients. The same can be said for higher level individuals who could become corrupt. An external audit is sometimes done to verify the authenticity of financial information that has been processed by high-ranking individuals. Formal open communication to mitigate these risks can be established by having an HR function within the organization framework or by having a clearly established chain of command that would also be in charge of workforce motivation to their subordinates.
But informal communication interfaces, within scope of the company, will allow management to view and understand inter-organizational relationships and also identify individuals who would be possible perpetrators. Team building and workshops are interfaces that the organization can use to assess risks that could come from the internal workforce.

Along with the formal fraud risk assessment (which is advised to be conducted on a regular basis if there were no anomalies that would incur changes within the assessment criteria) and direct interviews with the workforce the organization must understand that sometimes fraudsters use methods of intimidation in order to silence parties that would expose them. It is for this reason that there must be an anonymous reporting channel for fraud that should exist within the architecture of the organization. Individuals who are aware of fraud but do not with to be implicated in the investigation should have the option to report fraud anonymously to management in order to identify, assess and control the fraudulent eventuality.

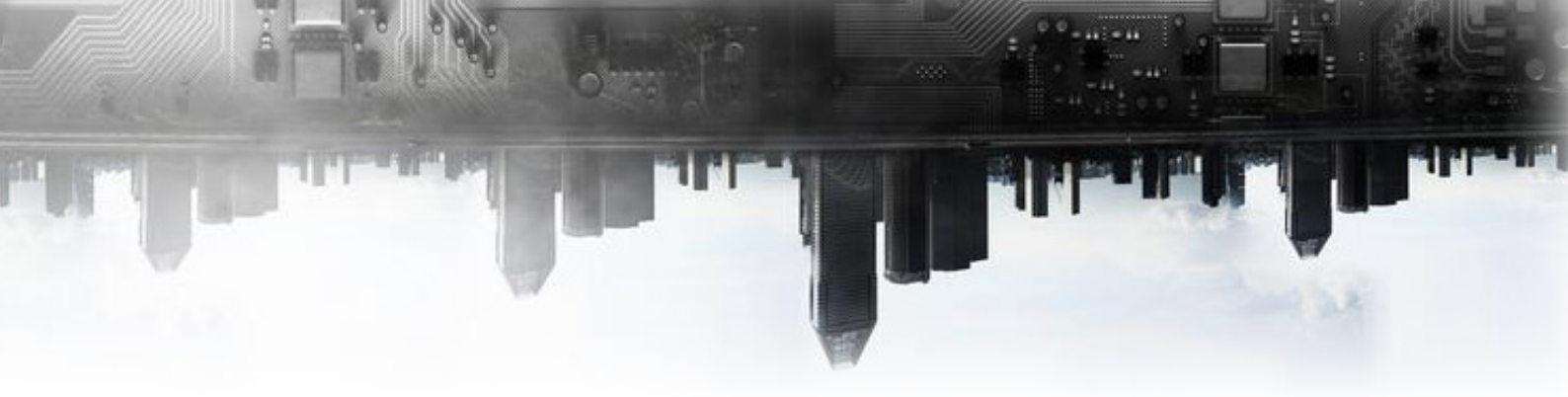
Individuals who take an outright stand against fraudulent activity within the organization can be referred too as whistleblowers. Those individuals are usually placing themselves at risk in order to report fraudulent activity to the company. It is within the best interests of the company to protect these individuals by allowing them anonymity during investigation or invoking controls that would assist in the safety of the whistleblower. Unfortunately, this cannot be extended outside of the jurisdiction of the organization (unless it is a matter that would take legal action and the police are involved against violent individuals) but the organization can take measures to ensure those individuals who will not tolerate fraud amongst the workforce can be protected and placated.

## Principles of an effective Fraud Risk Assessment

The principles of a fraud risk assessment involve looking at the business as a unit. although each organization will have a unique scope of what is contained within the fraud risk assessment there are several guidelines that give a basic framework of what the organization would have to have in place to make the fraud risk assessment an effective tool to combat fraud.

The fraud risk assessment must give descriptions of fraud risks and schemes in order to easily identify less impactful fraudulent activity. This is helped if the organization has applied segregation of duties and well-defined roles and responsibilities in the company. Along with stating outright the fraud risks that the company can succumb too it is vitality important to have an anti-fraud program in place to help educate the workforce to combat fraud at ground zero. When the fraud risks are identified the anti-fraud program of an organization can be tailor made to suit that company's interest. Each fraud risk must be listed as how it will impact the organization in terms of loss.

The second principle that is necessary for an effective fraud risk assessment is that all anti-fraud controls within the organization must be subject to review, this includes current controls that are in effect, preventative controls that could be implemented as well as any defective controls that are no longer in use. Robustly reviewing these aspects will lead to a more effective fraud risk assessment as the sustainability of those controls can be measured using the fraud risk assessment. This will be the tool that management uses to identify controls that are no longer effective or moot.



In addition to identifying fraud and listing the anti-fraud controls of an organization, the fraud risk assessment must also address the likely hood of fraudulent acts to occur and must plan ahead in order to deal with acts of fraud. When a fraudulent act has occurred, the organization is advised to always make a note of how large the likelihood is of the crime being repeated and what controls could be put in place to deter fraudsters from repeating those acts.

The fraud risk assessment needs to address the organizations responses to risks when they occur. This will include any actions taken to alleviate damages caused to the organizations internal controls as well as any legal action taken against persons in violation of the company's policies. These responses are important as that this will be the examples to the workforce of what would happen to persons violating the company's anti-fraud policies.

Fraud prevention and detection measures must be stated in the fraud risk assessment to ensure that investigations are carried out efficiently and according to company policy. Workers must never be allowed to feel targeted as fraud would affect all persons in the organization. All individuals are subject to investigation and nonconformance with this principle could lead to red flags surrounding certain individuals within the organization.

Consistent monitoring and reporting of anti-fraud controls allow management to assess the efficacy of their current fraud risk assessment. Simply doing a fraud risk assessment once a year will mean that within the year that is under review fraud could have taken place and no one would be any wiser until the assessment is being conducted. Such a scenario is frightening to consider if the organization made a payment to a "false" supplier and the monies could not be recovered after the initial fraud has been detected. Fraud risk assessments should be done regularly, depending on the nature of the organization, and must be subject to the closest level of scrutiny.

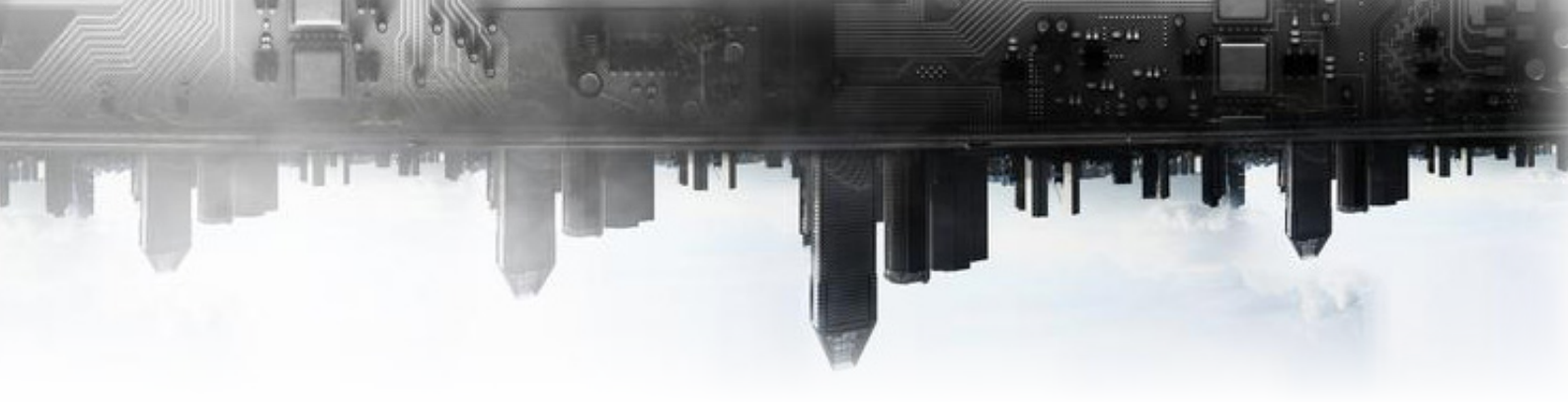
## Anti-Fraud Program

Along with the fraud risk assessment there needs to exist a culture of fraud awareness within the organization. Many organizations have workshops designed to help the workforce understand how fraud operates within the organization, but it is becoming more common place to have an anti-fraud program in place within the company. This program should make protocols to deal with the eventualities that would arise within the day to day running of the organization, for example a lower-level employee approving payments on a managers computer system. This is fraud, as it is a lower-level employee "digitally impersonating" their manager. Regardless of if no one gets hurt the business must have consistent policies in place that would define the roles and responsibilities of all individuals.

The anti-fraud program also needs to outline the reporting procedures of fraud, the protection offered to whistleblowers as well as the investigative and corrective action that the organization will follow if or when a fraudulent eventuality unfolds.

The fraud risk assessment falls under the scope of the anti-fraud program, but an effective fraud risk assessments needs to be consistently monitored and policy adjusted where controls are likely to fail. Understanding that fraud is not always financial fraud is an important principle in the fraud risk assessment. For example, employees are allowed to use expensive "general" equipment to work, but there is no checklist to say who is using the equipment at that time, in addition to that (as there could be fraud committed on the checklist) a digital clocking device would then ascertain which worker was working at a specified time or date.

This could be identified in the survey question as follows
*Please rate on a scale of 1-5, where 1 means never and 5 means always.*
*How often do you forget to write your name in the user log of x-machine?*



If the majority of the answers returned would be a 5 then using the fraud risk assessment, we can identify that identity fraud is likely to occur as workers can list those other workers were using the machine at a specified time. Another scenario would be that work was never completed but the workers had submitted a claim for hours worked and they had "forgotten" to log their time on the machine. A control that could be implemented and monitored is using a data system to unlock functionality of the machine and log the users time and identity.

## Ethics and Moral codes

The organizations controls can sometimes be lax in terms of the hiring process. It is a crucial component that the individuals who make up the majority workforce in an organization have strong ethical values that are implemented in their productivity output. But we do not live in a perfect world.

Sometimes the organization decided, inadvisably, to override its own controls by allowing individuals who propose a risk to the organization to be taken into the fold. This bad apple would have not only the opportunities to bypass externally oriented risk management controls but would influence others that the rewards for their discretions will be worth it. It is important that the Human Resource Functions implement the strictest controls possible to ensure that only persons whose moral compass is aligned with the vision of the organization are allowed to participate in the organization's bounty.
Although this is proven to be the case with most "redemption" arcs, there are still success stories of persons being influenced by the values within the organization and those that are shared within its workforce. That can be achieved by having employee workshops that teach employees the values of professional business practice. Having controls that allow anonymous reporting of suspicious activity these morally positive employees will directly be able to help identify possible risks within the organization.

Human capital risk is defined as the human skills, knowledge and ethical conduct component of operational risk and traditionally defined as the risk of an organizations human resources coming in the way of having a sustainable future in the market. Having a powerful and dynamic human resource business function in place, that acts as an incentivizing plan to envision productivity within the workforce. These incentives can be based on simple moral rewards for jobs well done, successful reporting of possible risks etc. The human resource function should ensure that an open culture of communication between the chains of command and relation within the organization exists to easily identify possible risk areas to be enforced by management.

The directorate of the organization has the opportunity to mandate policies that must be agreed to by employees. Employees who violate this "Moral Code" are subject to investigation or even termination if specific actions of discretion are defined within this code, thus the code can also act as the disciplinary guideline within the organization (Although these disciplinary measures must be within the scope of legislation).

Human capital risk now has an impact across the entrepreneurial spectrum, not just the outright misappropriation of assets or funds. In this day and age an organization's reputation and exposure is a direct lifeline to their sustainability, but if the organization suffers damage to that reputation it will lead to a potential loss of patronage. By having the following defined within the human resource function would greatly reduce human capital risk:

- Having adequate and thorough hiring protocols
- Having proper reporting functions and whistle blower policies in place
- Have a well-defined code of conduct and disciplinary documentation
- Having a digital asset policy to foster positive cyber practices between employees.

## Conclusion

It is never the strongest who survive, that archaic law of the jungle no longer applies in the day and age business world. Currently the consensus is that those who are the most adaptable are the most viable to survive. This is how the fraud risk assessment comes into play as a major trump that the organization can use to flush out fraud within themselves and their external locus.

The fraud risk assessment is crucial to stating and understanding the vulnerable areas of the business. Having an open culture about fraud awareness and an effective anti-fraud campaign will in the long run help an organization minimize their exposure to risk and fraud if it, and the policies and procedures that go along with it, are regularly updated, and improved.