The Mitigator

Editorial

"If you don't have the time to do it right, when will you have time to do it over?" — John Wooden.

"Getting it right the first time" is only attained through a continuous cycle of planning, doing, checking or evaluating and acting following best practices and strong methodology.

This will ensure the efficiencies required to meet and exceed expectations continuously.

Doing things right the first time, vastly limits the waste of time, effort and money . Ccorrecting faults resulting from doing tasks the quick and easy way, without proper planning and controlling quality does not make business sense at all.

OUR PARTNERSHIPShe

Aptitude Media partners with providers of solutions aimed at risk-based corporate governance, ranging from management system design, capacity building and implementation to practical technology-based solutions.

As an authorised partner of **PECB**, a certification body that provides education , certification, and certificate programs for individuals on a wide range of disciplines, we help professionals to get things right the first time by developing competence in various areas of expertise by providing valuable evaluation, certification, and certificate programs against internationally recognized standards.

this issue

And it's 2024!

With the brand new year still in its fledgeling stage, it makes sense to take a moment to contemplate what is lying ahead and get the ducks in a row right at the kick-off.

With all the well-wishing for 2024 done, the opportunity to make 2024 a great one beckons – depending on how it is approached from the onset.

It is of critical importance to make provision for robust, implementable contingencies and capacitating people to execute tasks.

As South Africa enters a pivotal year, it faces a confluence of risks that threaten its socio-economic stability. From the spectre of civil unrest to the shaky foundations of its state-owned enterprises, each carries the potential to exacerbate the others, creating a complex web of issues.

Crippling power cuts, volatile commodity prices and a challenging external environment have contributed to the country's weak growth performance. Real GDP growth is expected to fall sharply from last year.

South African realities contributing to this forecast are, amongst others:

- A major energy crisis due to the mismanagement of Eskom.
- Poverty, growing inequalities, high unemployment, social risk (crime, strikes)
- Inefficient public spending and corruption.
- Lack of foreign direct investment.
- Weak public accounts and state-owned companies.

South Africa ranks among the top 35 most dangerous countries in the world, according to the latest 'Global Peace Index' by the Institute for Economics and Peace. Out of 163 independent states and territories ranked according to their peacefulness, South Africa has come in at 130.

International security company G4S finds in its inaugural 'World Security Report' that South Africa will be the worst-affected country globally by security-impacting hazard disruption of energy supplies in the coming year. According to insights gathered from 1 775 chief security officers from 30 countries, 33% of global respondents flagged disruption to energy supplies as a concern, compared with 55% of South African chief security officers flagging this as a concern.

The second biggest security-impacting hazard among global participants is expected to be economic unrest related to stagnant economic growth or recession, which was flagged by 45% of South African chief security officers as a concern. Moreover, 41% of South African chief security officers agree that the risk posed by social unrest, such as protests, will remain a serious concern going into 2024.

The misuse of company resources or data remains a predominant internal threat, 43% of South African respondents believe misuse of company resources or data to be the predominant internal threat.

96% of South African companies rated internal threats to be affecting them in 2024, with some of the most impactful internal threats being internal fraud and misuse of company resources or data. South Africa rated the second-most affected nation in the world by internal fraud, following Kenya at 57%.

In terms of external threats, 32% of South African chief security officers anticipate trespassing to be a significant external threat to their organisations in the coming year, while 30% expect fraud to be a significant external threat. This compares with the global average of 20% for trespassing and 25% for fraud.

South African respondents are also more concerned about subversives (protesters, hackers or spies) as a genuine threat group for the coming year at 54%, compared with the global average of 50%. Loadshedding affects security systems, making companies and utilities more vulnerable to potential attacks.

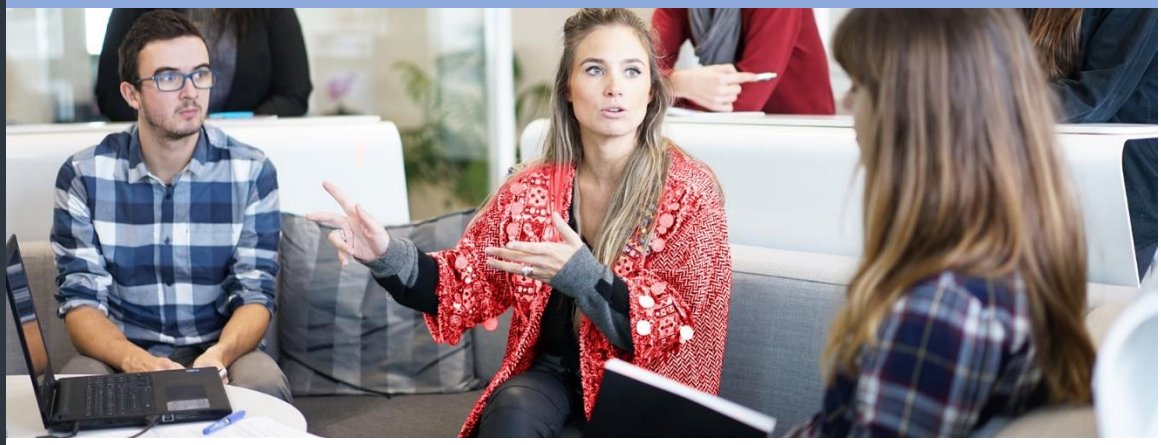
Conducting a Proper Root Cause Analysis

Root Cause Analysis is a well-known method to find the primary causes of a problem by sourcing a wide range of tools and techniques. By looking at the reasons of why a problem occurs, you can correct or eliminate the incidence of the underlying problem. A Root Cause Analysis tends to uncover issues such as faulty design and materials, failure of machines, human error, incorrect work instructions or procedures, among many other structural issues. Thus, its importance is paramount when attempting to evaluate the system and reduce or eliminate errors.

PECB Root Cause Analysis certification shows that you have the ability to pinpoint the causes of undesirable events and provide instant corrective actions, before they have an impact on other processes, systems or people. By having a root cause analysis infrastructure in place, you will be able to thoroughly analyze the situation, quickly identify the error causing factors, and set forth parameters to mitigate and repair them.

This will help you to create a culture of continuous improvement, and to assist your organization in increasing its productivity and decreasing its downtime. As you will be able to:

- Identify potential risks
- Solve problems more effectively
- Prevent the reoccurrence of problems
- Generate greater sales
- Increase productivity



R85 million compensation claim dismissed with costs

By André Jacobs

The critical importance of having a working Occupational Health and Safety Management System in place can not be underestimated.

André Jacobs, a seasoned health and safety practitioner at Aggregate Trading Solutions (Pty) Ltd, associated with Aptitude Media writes:

A certain company conducted accredited OHS incident Investigation training for supervisors in Nov 2015.

In 2016, Henry (not his real name) worked at a steel supply company in Cape Town as a spray booth operator for the epoxy coating of steel products. The OHS requirements entail a site-specific risk assessment and personal injury mitigation PPE, namely breathing respirators. On the day, Henry was overcome by inhaling fumes from the epoxy spray, collapsed and was found unconscious on site. First responders administered first aid resuscitation and revived Henry. Pictures were taken at the scene and later used as evidence for the case. EMS transported Henry to hospital and was admitted to ICU for recovery. Henry survived the incident and the medical report stated he sustained lung damage and blood poisoning.

A workman's compensation case was lodged with the Dept of Labor for medical expenses and loss of income. Henry left the company 3years later.

Six years later in Feb 2022, Henry`s lawyer lodges a civil claim for compensation at the High Court based on his current medical condition relating to an incident that occurred at work and that he is unable to breath without an oxygen tank, hence unfit to work for the rest of his life. R85 million is sought as compensation and loss of income due to ill health resultant from the on-site incident in 2016.

I returned to the company for Legal Liability training for managers on a Monday in May 2022. The management revealed the details of the case in class and stated that they were in a flat spin as the final arguments had to be presented by the Friday.

I reminded them that records had to have been kept of the incident. They informed me that the foreman had retired two years back who was the investigator of the incident. This foreman was in the class I had trained in 2015.

I recommended that the original case file be found, and that the investigator (now retired) be contacted.

The company had some documents, but over time had neglected maintenance of Safety File documents and in particular the incident reports & investigations.

Fortunately, the previous foreman (now retired) kept a copy of the incident investigation that he had conducted, with copies of the pictures taken at the time of the incident.

The pictures showed the incident scene from a distance and others of the surroundings at the time. One picture showed the employee in a collapsed position with his entire face covered in grey epoxy spray with a peculiar triangular-shaped clear-skinned spot the top of his bald head. This indicated that he had sprayed without correct use of the PPE mask and that it was on his head at the time of spraying.

This was presented in court and the case was dismissed with costs.

During the interview with the retired foreman, he made mention that he had applied the investigation principles & methods covered in the OHS training class, which I had conducted in 2015.

The company has since implemented **ISO 45001**, re-called the foreman from retirement and I was retained as the OHS Consultant.

André can be contacted at

+27 82 659 0026

or emailed at ***andre@safeti.co.za***

Cybercrime – a reality to contend with

Organizations worldwide are nowadays affected by the ever-evolving digital landscape and constantly face new threats and complex and sophisticated cyberattacks. There is a pressing need for skilled individuals capable of effectively managing and implementing robust cybersecurity programs to counter these threats.

South Africans and South African Businesses are also increasingly targeted by organised crime groups to obtain information and intelligence to plan online theft, including identity theft and information theft with the ultimate goal to gain financially illicitly.

Cybercrime cases are difficult to prosecute and, while there are good skills within police to deal with cybercrime, there are not yet enough people with the skills to develop and implement effective cybersecurity measures in businesses.

In their web site brief on cybercrime, the South African Police Service advises that "cybercrime is a fast-growing area of crime".

More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit "a diverse range of criminal activities that know no borders, either physical or virtual".

These crimes can be divided into the following three broad areas:

- Attacks against computer hardware and software, for example, botnets, malware and network intrusion
- Financial crimes and corruption, such as online fraud, penetration of online financial services and phishing
- Abuse in the form of grooming or 'sexploitation', especially crimes against children

Cybercrimes are committed by criminals using cell phone and internet connections. However, organised crime groups are becoming more and more sophisticated by the day and use advanced technology as well as psychological tactics to commit their crimes.

The modus operandi changes continuously according to the victim profiles and can vary from individuals with low technological literacy to businesses with advanced cyber security systems already in place.

It is imperative that businesses have the internal capacity to at least implement the fundamentals of an effective cybersecurity governance and understand how it serves as the backbone of a robust security strategy through practical approaches to identify, assess, and mitigate cybersecurity risks.

PECB's Lead Cybersecurity Manager training course guides individuals towards mastering the ability to implement and manage a cybersecurity program based on industry best practices. The PECB Certified Lead Cybersecurity Manager, will be made familiar with the fundamental cybersecurity concepts, strategies, methodologies, and techniques utilized to effectively establish and manage a cybersecurity program based on the guidance of international standards and industry best practices for cybersecurity.

This training course empowers participants to enhance their organization's readiness and resilience against cyber threats.

Participants will be well-prepared to support their organization's ongoing cybersecurity efforts and make valuable contributions in today's ever-evolving cybersecurity landscape.

Become an associate and join our network

How we work:

Aptitude Media seeks to optimise best practice implementation by soliciting input from a variety of associates to the benefit of a range of beneficiaries in both the private sector and the public sector.

We achieve this by sharing experience, knowledge and expertise on a mutually beneficial commercial basis, following a "per project, per assignment" business relationship approach.

We believe that, by networking amongst experts in various fields, we can collectively add value to not only the wide range of clients currently serviced by Aptitude Media, but also those of our associates, who trade as separate business entities in their own right.

Intellectual property and business interests are guarded as highest priority, with formal non-disclosure and restriction of trade agreements finalised before every business engagement.

EYE ON IT
General Election 2024

"As we edge closer to the general elections, political tension, compounded by labour disputes and budgetary constraints is palpable", writes Volker Von Widdern, Head of Strategic Risk at Riskonet

Brought down to business level, the year ahead for South Africa is fraught with challenges, but it is also ripe with opportunities for transformative change.

By adopting a multi-dimensional approach that encompasses business and corporate governance reforms, businesses can not only navigate these turbulent waters but also emerge stronger and more resilient.

The path ahead is complex, but with collective will and strategic action, stability and growth are within reach, Volker von Widdern writes.

Much of this lifting will be done by the risk community and it is imperative that risk professionals in both public and private sectors, analysts, and strategists come together to provide insightful foresight and pragmatic solutions.

His advice is to step forward and share expertise. Engage actively in policy discussions, contribute to strategic planning, and help in crafting robust risk mitigation frameworks. Risk practitioners are not just to predict and warn, but to be active architects in shaping resilient companies and a resilient South Africa. This includes not only identifying vulnerabilities but also highlighting opportunities for growth and stability.

There is a dire need for innovative thinking and collaborative efforts. By sharing knowledge, resources, and best practices, we can drive the creation of more resilient systems and businesses.

Continuous Professional Development

"*Continuing professional development (CPD) is defined as learning experiences which help you develop and improve your professional practice. This can include building on your strengths, as well as developing yourself where you have capability gaps".*

PECB AUTHORIZED PARTNER

The Mitigator

Your contributions are welcome

Upcoming Training and Certification Events

Business Continuity Management

Protect, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise. With a business continuity management system, your organization is prepared to detect and prevent threats. ISO 22301 enables you to respond effectively and promptly based on the procedures that apply before, during and after the event. Implementing a business continuity plan within your organization means that you are prepared for the unexpected. Business continuity plans assures that your organization will continue to operate without any major impacts and losses.

Root Cause Analysis

Root Cause Analysis is a well-known method to find the primary causes of a problem by sourcing a wide range of tools and techniques. By looking at the reasons of why a problem occurs, you can correct or eliminate the incidence of the underlying problem. A Root Cause Analysis tends to uncover issues such as faulty design and materials, failure of machines, human error, incorrect work instructions or procedures, among many other structural issues. Thus, its importance is paramount when attempting to evaluate your management system and reduce or eliminate errors.

Occupational Health and Safety Management

To mitigate the risk and hazards in the workplace, organizations must prioritize the health and safety of their employees. Organizations and individuals operating in any industry must collaborate to achieve the same goal, which is to reduce as much as possible the number of accidents that lead to injury or health-related issues. This course will enable you to comprehend internationally recognized practices that are intended to improve the working conditions and guarantee the well-being of employees

Risk Management

Risk is present in every aspect of our life, from mundane everyday activities such as choosing a route to work, to complex corporate decisions such as opening a manufacturing plant. Knowledge and implementation of the ISO 31000 standard enhances the understanding of risk and its nature, which leads to the creation of methodologies and approaches that enable individuals and organizations to make accurate decisions based on logical reasoning.Risk management will empower you as a manager to get involved in the nitty gritty of the management task. Systems do not manage your company, you do.

Crisis Management

A crisis is an abnormal event that threatens the continuity of an organization's operations and may even lead to its collapse. These events may have natural causes or may be man-made, e.g., natural disasters, environmental issues, terrorism, cybersecurity breaches, and employee misconduct. A crisis can occur abruptly or may emerge from small incidents that have not been addressed or have been managed inappropriately. By improving their crisis management capability, organizations not only prepare for and prevent crises, but they can also manage crises more effectively and learn from them by identifying opportunities for improvement. The ISO 22361 standard provides guidance for organizations to develop, establish, maintain, monitor, and continually improve a strategic crisis management capability. In addition, it outlines principles and practices needed to identify and manage a crisis.

The Mitigator, all about knowledge sharing related to corporate governance, cordially invites contributors to this newsletter

Full acknowlefgement willl be given for all contributions placed.

The editor reserves the right to decide on placements. Any edited versions of contributions will be submitted to the contributor prior to placement.

Contributions can be emailed to info@aptitudemedia .co.za

-Ed