ISSUE ONE | JUNE 2020

The RiskEcho

An Insightful Risk Management Publication by the NSSF

Inside

Interview with NSSF MD, Mr. Richard Byarugaba

Richard Byarugaba, NSSF's Managing Director sits down with Our Interviewer.

Innovation Risk- Navigating The Grey Areas

Innovation risk is like a double–edged sword, full of uncertainties yet it can be a game changer.

Understanding Fraud Dynamics

Nearly every organization has experienced fraud at some point in time. Here's what you can do

Welcome

I am truly excited to introduce to you our first edition of The Risk Echo magazine, which tries to demystify the concept of risk and risk management.

Every organization and indeed, every individual faces several risks the management of which draws the line between success and failure. In the words of Gary Cohn, “If you don’t invest in risk management, it doesn’t matter what business you are in, it’s a risky business.”

However, in practice risk management is one of the areas most organizations do not pay serious attention to, and yet, as mentioned above, the way risks are managed determines whether an organization and indeed an individual succeeds or not.

The question then is, why is it that something so important, to the extent that it determines your success or failure, is not taken as a matter of priority? To this and many more questions, find the answers in this Risk Echo magazine.

I believe you will find it an exciting piece to read, because it is educative and informative; we have covered exciting topics such The future of pension funds, Understanding risk a in a broader contest, Corporate lifestyle dilemma, Cyber response plan, how your risk appetite influences your decisions, and a lot more.

“If you don’t invest in risk management, it doesn’t matter what business you are in, it’s a risky business.”

But most importantly, we bring you an exciting interview with Richard Byarugaba, the Managing Director of the National Social Security Fund (NSSF).

Richard is an accomplished accountant, a fellow of the ACCA, a Certified Public Accountant (Uganda). He holds an MBA from Edinburgh Business School (UK), a Management Diploma from Henley Management College (UK) and a Bachelor of Science degree in Statistics and Economics from Makerere University.

Richard has wealth of experience spanning over three decades in financial institutions. As you may be aware, Richard has been at the helm the NSSF since 1st September, 2010, and has seen the Fund transform from one of the most corrupt institutions in Uganda to now, one of the most coveted organizations in the country, with the largest balance sheet, worth UGX 11.338 trillion as at 30–06–2019.

He explains the role of risk management and why it is important to set the tone from the top.

Finally, I take this opportunity to thank you for having chosen to read The Risk Echo magazine, I hope it will enhance your appreciation of risk and risk management.

To those who have contributed to this publication in one way or the other, many thanks.

Edward Senyonjo
Head of Risk, NSSF
MBA, FCCA, CPA, BCOM.

CONTENTS

Interview

06 **Interview with NSSF MD, Mr. Richard Byarugaba**
Richard Byarugaba, NSSF's Managing Director sits down with Our Interviewer.

Leadership & Good Practice

10 **How your Risk appetite affects your decision-making**
Risk appetite defines the sphere of decision–making in a risk environment.

12 **Risk Management, a Business Enabler**
An analogy to help explain risk management; Why does a Ferrari have brakes?

13 **A Risk Manager in Leadership**
Why a risk manager needs to develop leadership skills.

Make A Difference

14 **Innovation Risk; Navigating the Grey Areas**
Innovation risk is like a double–edged sword, full of uncertainties yet it can be a game changer.

16 **How Effective is your Cyber Incident Response Plan?**
Every organization is a potential candidate for cyber–attack; Learn how to protect yourself

Expand Your Horizon

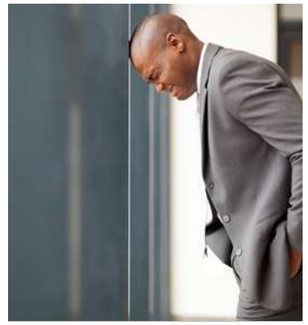
18 **Understanding Risk in a Broader Context**
The word "danger" comes to mind whenever risk is mentioned, but risk goes beyond that

22 **The Future of Pension Funds in the Face of Declining Interest Rates on Bonds**
With a steady decline in global interest rates on bonds, Pension Funds must begin to consider alternative investments

Pg. 28

Pg. 06

Pg. 36



Pg. 16

Pg. 14

Pg. 18

24 **Understanding Fraud Dynamics**
Nearly every organization has experienced fraud at some point in time. Here's what you can do to minimize chances of fraud

28 **Risk Hedging with Forward Contracts**
A hedge consists of taking an offsetting position in a related security such as futures, forwards, options & swaps. Find out how they work.

30 **Risk Management: A Tool for Performance Manageent**
Achievement of organisational objectives is greatly influenced by how well risk and performance are managed.

Crisis Management

32 **COVID-19: An Effective Crisis Management Plan Can Make a Difference**
What we can learn from Singapore and Taiwan's effective COVID–19 crisis management.

Trends & Lifestyle

34 **Our Health is a Function of our Choices**
What we do or not do has a significant impact on our health

36 **The Corporate Lifestyle Dilemma**
If you have worked in the corporate world, you will agree that corporates often try to project an image of class.

Trivia

38 **Test Your Risk Knowledge**

If you do not investment in risk management, be prepared to harvest huge losses.

Richard Byarugaba, NSSF Managing Director

– An Interview with NSSF Managing Director –

Setting the Right Tone at the Top

Setting the right tone at the top is extremely important, especially through actions of the leaders, because actions speak louder than words – Richard Byarugaba, NSSF's Managing Director explains to our Interviewer.

Before you joined the NSSF, it was bedeviled with corruption and embezzlement of funds. What is it that you did that was able to transform this institution into one that is devoid of corruption and coveted by everybody?

First of all, we streamlined our processes, policies and procedures, enhanced our recruitment process to ensure that we recruited people of high integrity, as well as improving staff warfare.

We also built robust risk management and internal control systems, which ensure that risks are constantly monitored, and controls are assessed regularly, to identify control weaknesses and address them timely and effectively.

I understand the Fund adopted an Enterprise Risk Management (ERM) model ever since you were appointed the MD. How has ERM contributed to the transformation of the Fund?

The introduction of Enterprise Risk Management helped us to break the silo mentality and build a culture, where risk is viewed as part and parcel of the daily business activities that have to be managed in order to achieve business objectives across the Fund. The effectiveness of risk management is one of our of key performance indicators at corporate, functional and individual levels.

The starting point for effective risk management is to define the organization's risk appetite. To what extent does the Fund's strategy align with its risk appetite?

We have a well–defined and documented risk appetite framework that guides our strategic decisions. We have set risk appetite limits, at strategic and operational levels that act as boundaries for the decisions we make.

This is mainly reflected in our strategic asset allocation, where our appetite is highest for fixed income (80%), equity–15% and alternative investment–5%. For the obvious reason that the risk associated with fixed income is low, but also the returns on fixed income assets are relatively good.

Richard Byarugaba (C), (NSSF, Managing Director), Patrick Ayota(L), (NSSF, Deputy Managing Director) and Edward Ssenyonjjo (R), (NSSF, Head of Risk)

Proponents of risk management assert that the difference between success and failure is effective risk management. Do you agree with that assertion and to what extent?

To a great extent, yes, because achieving your objectives largely depends on how effectively you manage the risks associate with the objectives.

In many organizations the role of risk management is not well understood. How is the culture in the Fund regarding understanding and appreciation of the role of risk management?

When we conducted a risk culture review by an independent firm in 2018, we found out that the risk culture in the Fund is at the maturity stage on the risk management maturity model.

Since the introduction of ERM (Enterprise Risk Management), a lot of effort has been put in inculcating the culture of risk management across the Fund.

If you do not investment in risk management, be prepared to harvest huge losses.

One of the key elements of a good risk management culture is setting the tone from the top. How is this practiced in the Fund?

Setting the right tone at the top is extremely important, especially through actions of the leaders, because actions speak louder than words. At the Fund, risk management is well positioned, right from the Board, Executive management and at departmental level.

With changes in political, economic, social and technological environment, the risk land scape is increasingly becoming more unpredictable. How is the Fund prepared to counter potential risk exposures?

The Fund has, over the years, developed adequate capacity, in terms of human resources, systems, and policies and procedures to manage any risk exposures. We have demonstrated our resilience from time to time, as we have been able to generate a reasonable return for our members, which has always been at least 2% over and above the 10–year average inflation rate

As the Managing Director of the largest financial institution in Uganda, what are the top two risks that keep you awake?

i) COVID–19

In the short and medium, I am so concern about the effects of COVID–19 on the entire business and our staff. Stocks, which are part of our investment portfolio, have plummeted; this will result in significant capital losses.

Additionally, a number of our employers have been greatly affected and their future is uncertain. This affects our cash inflows and therefore, the funds available for investment. No one is sure when and how this crisis is going to end.

ii) Cyber–attack.

Cyber risk is increasingly becoming a global threat to governments, organizations and individuals. Although we have built a robust security system, cyber risk is highly dynamic and unpredictable.

Your last thoughts on risk and risk management?

If you do not invest in risk management, be prepared to harvest huge losses.`

Edward Senyonjo
Head of Risk,
National Social Security Fund

How your Risk Appetite affects your Decision-Making

Risk appetite defines the sphere of decision–making in a risk environment.

Risk appetite can be likened to the appetite for food. Appetite is simply the desire to eat, often times due to hunger; although food that appears delicious with a tantalizing scent can stimulate appetite even in the absence of hunger. The word appetite can be used to refer to the desire for different things e.g appetite for soccer, appetite for politics, sex, etc.

From a risk perspective, risk appetite is the nature and level of risk an organization is willing to accept in pursuance of its objectives. When risk appetite has been defined and documented, it is then described as a risk appetite statement, which communicates to the stakeholders the extent to which the organization is willing to accept risk and the nature of those risks.

A risk appetite statement is a high level statement that considers broadly the level of risks that management deems acceptable in achieving organizational objectives.

Usually risk is associated with the actions we take, and the actions we undertake normally depend on our risk appetite. For instance, if a new technology is introduced, not everybody embraces it immediately; some will play wait–and–see. The ones that embrace the technology immediately are considered to be risk–aggressive or risk takers, while the laggards are considered to be risk averse. Therefore, the choice between adopting the technology immediately or later, is informed by the extent to which the individual is willing to take or accept risk, which is risk appetite.

Risk appetite is the nature and level of risk an organization is willing to accept in pursuance of its objectives.

Risk appetite is quantified in terms of risk tolerance limits, which act as boundaries for decision–making. For each key decision, the question to ask is, “is this within my/our risk appetite? Tolerance limits are metrics that show the level of risk the organization is willing to accept/tolerate.

An organization’s risk appetite is influenced by a number of factors, including: expected returns, statutory/regulatory influence, stakeholder influence, etc. For an individual, his or her risk appetite can be influenced by cultural and religious backgrounds, as well as peer pressure, among others.

Generally speaking, risk appetite is inversely related to the level of risk. The natural instinct is to avoid risk, especially high risk. However, if the benefits are expected to be high, there is always an inclination to seek to take the risk, thus the saying, “the higher the risk, the higher the returns”, is true.

Defining a risk appetite and monitoring to ensure that it is complied with, minimizes surprises/unexpected losses.

Joseph Biryahwaho
Head of Risk & Internal Control,
FINCA Impact Finance

Risk Management, a Business Enabler

One of the analogies that best explains my mindset towards risk management, is the analogy of why a Ferrari has brakes.

The analogy is from a seemingly random question that was asked at one of the Ferrari customer town halls, and the exchange went something like this;

Question: Why does a Ferrari have brakes? Answer (customer): So it can go really fast... Now, I bet that is not the first response you would get from most people if you asked why a car has brakes. The more likely responses would go along the lines of safety, protection, safeguard etc. And yet, an iconic automobile like a Ferrari, is at its most glorious moment while 'flying' at speeds beyond 150kph. So, one would argue that a world class braking mechanism, only serves to secure such an experience, and allows the Ferrari to be the iconic machine that it is.

Apply the same question to risk management, by asking; why is risk management necessary? And the likely responses would go along the lines of; safeguards, mitigation, vulnerability management, detection and prevention, etc. It is also then, a pity that many business owners and leaders have come to expect as much from their most senior risk custodians and advisors.

Well, if I can attempt an intervention against this perspective of risk management, I would urge a re–think by the risk practitioner.

I would urge the risk practitioner to harness and leverage his/her technical risk management expertise to intimately understand the most important commercial aspects of his/her organization. This enables him/her to focus on enabling the success of the organization, rather than just avoiding failure.

A risk manager that enables, oils and calibrates the success levers of an organization, offers a distinct value beyond one that is fully, even if promptly, advised the organization of potential pitfalls to avoid, but goes little further than that.
The key questions you should constantly ask yourself, as a risk manager, include the following;

i) Do I understand the business I am supporting, enough to manage it?

ii) Is my risk management strategy directly supporting the success of that business?

iii) What are the upside risks the business could exploit?

Understanding intimately the business you support, allows you to offer risk management solutions that directly support its success. Part of the risk management solutions you should look to provide is identifying upside risks.

An upside risk is where the business stands to get better outcomes than the benchmarks it has set. There is almost no business that doesn't have upside risks. An example could be the business setting a very conservative risk appetite for a product or economic sector, due to limited skill, inadequate technology, or inherent risks in the product/sector. This presents an upside risk, especially if the product/sector carries considerable potential for returns.

In such a scenario, the risk manager should be able to identify mitigating solutions that if implemented would unshackle the business' appetite. These could include but not limited to; the business partnering with third party entities on a risk sharing basis, outsourcing certain technologies that the business has insufficient skills to maintain/deploy, and phased deployments, as the organization tests and learns, among others. Solutions like these coming out of the risk management function should not be beyond reality.

The good news though, is that this rebrand or re–think of risk management need not require a change of tools, rather a change in the application of them. From risk appetite setting, to risk identification and control, to stress testing– all these tools and practices are integral to the operations of any organization.

However, using them to only identify pitfalls to avoid, and setting caps and limits to commercial aspirations, would be to limit your organization's potential for success.

So, I am led back my 'Ferrari brakes' analogy, and leave you with these questions; as a risk manager.

i) Do you give your organization the courage and confidence to thrive?

ii) Do you exploit upside risks enough?

Nigesa Diana Mboga
Risk Management Consultant
BA DevEcon, PRM

A Risk Manager in Leadership.

There is tendency for risk managers to concentrate on building their technical skills and ignore leadership skills.

The ability to influence others is very critical in risk management. A risk manager should be a good communicator, with ability to influence others, particularly executive management. This is because, the role of a risk manager is to identify, measure and communicate different types of risks and possible mitigation measures. That means, the implementation of risk control measures is undertaken by other stakeholders in the organization, who are usually referred to as risk owners.

The risk manager has the responsibility of ensuring that the work of mitigating risk is accomplished through others, which is key facet of leadership. The risk manager therefore, needs to strike a balance between technical competence and leadership ability.

Risk management is one of the concepts that are not well understood, and matters are made worse with the ever–changing environment, fueled by technological innovations, such artificial intelligence, block chain, big data, machine learning, inter alia.

If the risk manager employed the same analytical skills to understand the needs of his/her stakeholders, and put them into consideration when developing risk management strategies, he/she would be in a better position to effectively communicate with them for better understanding of risk management.

The risk manager needs to examine himself/herself by asking simple questions such as:

i) How effective do I communicate?

ii) Is it possible that I am using written mode of communication for a team that does not like to read?

iii) Am I igniting the desire for the team to participate in the change (risk culture) that I desire to see?

In conclusion, although the burden of developing a positive risk culture lies with everybody in the organization, effective leadership by the risk managers is very critical in developing a common understanding of risk and risk management, adoption of appropriate risk management practices and setting of the right tone at the top.

Michael Sendiwala
Investment Risk Manager,
National Social Security Fund

Robert Muwanga
Innovation Superviser,
National Social Security Fund

Innovation Risk – Navigating the Grey Areas

Innovation risk is like a double–edged sword, the journey itself is full of uncertainties and questions with no clear answers, and yet if handled well, can be a game changer for any organization.

Traditionally, the approach in many organizations has been to take a risk aversion approach towards innovations, as these were perceived to bring uncertainties that could affect the organization's bottom line. Innovation was viewed as an unnecessary cost to the business, rather than an opportunity to exploit.

Without innovation, especially in this contemporary dynamic world, where survival of the fittest is the order of the day– "man eat man",
a number of companies that are not taking innovation seriously have collapsed or are on the verge of collapse.

Embrace innovation but...

Today, the risk aversion approach to innovation is increasingly becoming archaic. Innovation has become centerfold in the boardroom, with the board taking an increasing role of overseeing new business development and its elements of experimentation.

In a report looking at the top 1000 global companies by Strategy + Business (2018) , research and development spend increased by 11.4% to $782 billion in 2018, reflecting the deep interest organizations across all sectors are putting in innovation.

Five Global Innovations Taking the World by Storm

1. Artificial Intelligence
AI based virtual assistants are becoming more popular than ever before and consumers are widely accepting AI–powered services. By 2030, the AI market will have surpassed $40 Billion.

2. Advanced Analytics
With growing volumes of data, there's growing need for smart, advanced analytics. The coming years will see a massive rise in data analytics as a service.

3. 5G Technology
Soon enough the breakthrough 5G technology will take over 4G. With faster speeds it is expected to deliver greater productivity with multi–gigabits per second.

4. Blockchain
Blockchain is the technology designed for accounting and verification of digital currencies (e.g bitcoin). It's expected to save infrastructure costs by about $15 Million in the next few years

5. Augmented Reality
Apart from gaming, Augmented reality is being actively used in 3D viewers, reality browsers etc. to deliver a wide range of experiences with expected revenues anticipated to hit $659 Million by the end of 2021

...beware Innovation Risk

One of the key success factors for innovation is, comprehensive identification and management of the associated risks.

Many companies that innovate without proper risk controls, experience hard times. The recently challenging innovation was in the aviation industry ; The Boeing's 737 Max innovation that led to a number of plane crashes, including the Boeing Lion Air in Indonesia and the Ethiopian Airlines plane (Boeing) on 29 October, 2018 and 10 March, 2019 respectively, that killed all passengers on board and the crew.

According to the investigators, that software, which is designed to help prevent the 737 Max from stalling, was faulty– it repeatedly pushed the plane's nose down, leaving the pilots fighting for control.

The report showed that there were incorrect assumptions about how the MCAS controls system would behave.

The frequent fatal plane crashes affected Boeing to the extent that the company had to ground all the affected planes. Consequently the plane orders dived very deeply after reports emerged of the existence of the MCAS system which was a major factor in the two crashes yet little stress tests/training seems to have been done.

Managing Innovation Risk

For an innovation program to succeed, there is need to pay special attention to potential risks. The mitigation strategies below can go a long way in addressing the potential risks to innovation:

Transparency of the entire innovation journey.
Of course the mechanics have to be patented in order to derive value of the investment, but you must open up to a confined group, especially your staff, to allow for positive criticism during the testing period. An open environment where views of everyone are considered can help to identify some critical areas which need to be fixed.

Quality assurance and risk assessments
Right from the ideation stage to the launch day, quality assurance and risk assessments have to be embedded in the innovation program.

Align the organization's innovation program with corporate strategy
To maximize buy–in from all levels of the organization – from the Board to Senior Management, ensure innovation efforts align with the needs of the organization's strategic vision. Investing in innovative solutions, just because they cutting– edge, but which do not solve current and/or future business problems), result in wastage of resources and erosion of shareholder value.

Adequate resources for innovation
Innovation should be facilitated by a dedicated team that is adequately financed and supported by cross–functional talent. Without a dedicated team and budget, it will prove difficult for an organization to successfully execute an innovation program.

Program structure
An Innovation program needs a small and agile team, with clear responsibilities and KPIs, and where progress is measured regularly.

A strong innovation leader is also needed to steer the innovation program, win support within the organization's ranks, and remove obstacles that can cause the program to stall or fail.

Break silos and encourage heterogeneous teams
With diversity, comes an increase in the quality of ideas generated. Being able to pool opinions, suggestions and experiences allows the creation of solutions that can solve business problems in an increasingly creative way.
Though homogenous teams are known to enable deep subject matter expertise on a given opinion, it is also known to reinforce biases and close out views that may diverge from the known norm.

How Effective is your Cyber Incident Response Plan?

Stephen Babigumira
Information Security Officer,
National Social Security Fund

Every organization is a potential candidate for cyber–attack; as a matter of fact, the question is no longer whether but when will the attack happen?

Due to the dynamic environment, characterized by intense competition, organizations are always confronted with a need to continuously explore new possibilities such as information technology innovations in order to survive or grow.

Information technologies (IT) have become a major driver of business efficiency and competitive advantage in the modern world. As such, companies are investing heav–ily in IT, with an anticipation of reaping the benefits of reducing costs, improving performance, productivity, service delivery, customer satisfaction and gaining a com–petitive advantage. As well, governments are implementing information technology initiatives to extend their services to all citizens, increase revenue collection, and strengthen their national security infra–structure, among others.

However, the same technology that brings us all these great benefits, makes organi–zations vulnerable to cyber incidents such as data breaches, Distributed Denial of Services (DDOS) etc. Every organization is a potential candidate for cyber–attack; as a matter of fact, the question is no longer whether but when will the attack happen.

A cyber–incident can expose your organi–zation to prolonged service down time, loss of revenue, fraud, inter alia, consequently resulting in reputation damage.

In a bid to protect valuable information assets against adversaries, companies have invested heavily in information securi–ty tools such as next generation firewall, Intrusion detection systems (IDS), Intrusion prevention systems (IPS), Security Incident and Event Management (SIEM), Data Loss Prevention (DLP) tools etc. Some companies have ended up creating an empire of tools, not to mention the fact that some of these tools just end up on the shelves, without being utilized effectively due to various reasons such as lack of skills to operate them. This provides an opportunity for the hackers to strike.
Although, even for those organiza–tions that are using the tools there is no guarantee that they will be immune from cyber–atacks, as the attackers are equally smart to be able to bypass the security systems.

Determined adversaries like hacktivists and state sponsored Advanced Persistent Threat's (APT's) will still find a way of bypassing these defense lines with highly sophisticated attacks or by exploiting zero–day vulnerabilities. Nonetheless, an organization that is ill–prepared is at a greater risk of a successful attack.

Therefore, your organization should think beyond protection to response. A Cyber Security Incidence Response Plan (CSIRP) would do a great deal in preparing your organization to respond and reduce the im–pact of a successful breach. This plan de–fines the breach, roles and responsibilities of the (Cyber Security Incident Response Team) CSIRT, tools, steps to be taken to ad–dress a security incident, how the incident will be investigated and communicated, notification requirements etc.

Surprisingly, most organizations do not have cyber incident response plans that can quickly spring them into action when an incident occurs. In the third annual study on the cyber resilient organization by Ponemon Institute and IBM Resilient, 76% of the or–ganizations that participated in the research said they lacked a formal cybersecurity incident response plan (CSIRP) that is applied consistently across the organization. Yet among those who had a CSIRP, 44% of respondents said they had not reviewed or tested the plan.

It is also true that some organizations develop cyder–incident response plans for purposes of compliance, only to be kept on the shelves to gather dust. This obviously gives them false confidence that they have an effective plan yet its obsolete and not fit for today's highly sophisticated attacks and highly experienced attackers.

The true strength of the CSIRP lies in regularly testing it. Cyber security drills will ensure your team knows what to do, when to do it, and who does what, without wast–ing precious time on what steps to take.

The drills will also act as a training op–portunity for your team to improve their capabilities in responding to the latest attacks. Like the saying goes "Practice makes perfect".

Practice your incident plan as much as you can to reap its benefits. You will not be able to execute your plan swiftly if you don't re–view/test it. When it comes to a cyber–in–cident, time is of essence; the more time the adversary has access to your network, the more damage he causes to you.

Therefore, your response plan should be triggered and executed at the speed that will enable you to limit the extent and re–duce the impact of a successful attack.

An effective cyber incident response plan should encompass all plausible attack scenarios, which should be simulated from time to time, and performed by a multi–disciplinary team, comprising Infor–mation Security, IT, Audit, Risk, Communi–cations and Legal specialists. Each of these will have an important role to play.

For example, the communications personnel will have to manage your correspondences and updates with the public or affected members, whereas the Legal staff will prepare for any suits lodged against your organization and ensure that you remain compliant with the applicable regulations of the country, when responding to a breach.

The Risk and Audit teams can assist in formulating scenarios and conducting business impact analysis.

A regularly tested cyber security incident plan is an invaluable asset for your orga–nization, it will go a long way in minimizing losses and protecting the image of the organization. It can be the difference be–tween success and failure in managing an attack. The 2019 cost of data breach report by Ponemon Institute and IBM, indicated that having a cyber–incident response team coupled with regular testing of the cyber incident response plan, reduced the costs of data breach more than any single security process. The report further indicated that extensive testing of the CSIRP reduces the total cost of a data breach by an average of $320,000 from the average cost of $3.92 million.

Therefore, don't wait for your organization to be counted among those that didn't do enough during and after a breach, pick up your plan from the shelves, dust it off and test it. If you do not have one, this should be your immediate priority this year. Nobody is immune to a cyber–incident, but the ill–prepared can be easily be put out of business.

Seven steps to an effective Cyber Security Incident Response Plan (CSIRP)

Step 1: Conduct a complete risk assessment.
The primary purpose of a risk assessment is to determine the likelihood and severity of risks in critical areas.

Step 2: Identify key team members and stakeholders
Appoint a cross–functional cyder–incident response team, including key decision–makers, such as senior managers; with clear roles and responsibilities.
As far as practical, the plan should include external key stakeholders.

Step 3: Define security incident types
Come up with different potential incident scenarios and analyze their impact on the business, well as determining appropriate strategies on how to deal with them in case they happen.

Step 4: Inventory resources and assets
Your company has systems and resources – create record and create an inventory of these resources in the response plan.

Step 5: Plan heirarchy of informaton flow
Take a look at the assets above. What are the steps that need to happen to execute different processes.

Step 6: Prepare variety of public statements
Security events can seriously affect an organisations reputation. Plan a variety of public relations statements ahead of time.

Step 7: Prepare an incident event log
During and after a cybersecurity incident, you are going to need to track and review multiple pieces of information – use a log.

Edward Senyonjo
Head of Risk,
National Social Security Fund

Understanding Risk in a Broader Context

Ordinarily what comes to mind when the word risk is mentioned, is “danger”

Indeed, the Oxford learner’s dictionary defines risk as the possibility of something bad happening at some time in the future or a situation that could be dangerous or have a bad result, while Merriam–Webster defines risk as a possibility of loss or injury–peril.

What is common to both of these definitions and many others, is the reference to risk as a possibility of undesirable outcome or effect. It should be to pointed out that the concept of risk is about the future– risk lies in the future, it is therefore, associated with uncertainty. If a loss or an injury, as mentioned in the definitions of risk above, has occurred, it is no longer a risk. This brings me to the technical definition of risk as spelt out in ISO 31000 Risk Management Principles and Guidelines. According to ISO 3100 Risk Management Principles and Guidelines, risk is the effect of uncertainty on objectives and an effect is positive or negative deviation from what is expected. The key words in this definition are: Effect, Uncertainty, Objectives, Positive or negative deviations.

Every individual or organization has objectives, and the objectives are set in an environment of uncertainty because they are set to be achieved in the future– no one sets objectives for the past. However, it is not always the case that the objectives are achieved, as a matter of fact, we always achieve less objectives than we intend to. The reason why some objectives are not achieved is that the effect of uncertainty on the objectives is negative.

Therefore, in risk management we are more concerned with the negative aspect of risk because this erodes value of the organization.

In the context of the organization, it is important to manage both aspects of risk– positive (opportunities) and negative (danger/threats). Opportunities are usually pursued by risk–taking functions such as operations, IT, investment, etc, while the “dangers” are the preoccupation of the risk–control functions such as risk management, audit, compliance, etc.
A clear separation of roles between risk–taking functions and control functions is important to avoid conflict of interest. For instance, if a loan manager’s performance is measured based on the size of the portfolio, he/she will be tempted to use aggressive methods to increase the size of the portfolio so as to attain high performance scores at the expense of credit risk control measures.

However, if credit risk control lies with another independent department, this anomaly will be minimized, as this creates effective checks and balance.

“According to ISO 3100 Risk Management Principles and Guidelines, risk is the effect of uncertainty on objectives and an effect is positive or negative deviation from what is expected.”

That is not to say that you create a “Chinese” wall between these two departments; the two departments can work collaboratively and coherently so as to attain the overall organizational objectives, which are impacted by risk. The risk–taking functions are the first line of defense.
Using the risk management framework designed by the second line of defense (risk management), the first line of defense can prevent, detect and control risks.

The third and last line of defense is offered by internal audit, who take a retrospective approach to review executed transactions for consistence with internal control measures, and provide assurance on the adequacy and effectiveness of the internal controls.

It is important to note that an organization’s approach to risk is influenced by management attitude towards risk.
An individual’s or a group’s attitude is influenced by perceptions which are in turn influenced by many factors, including cultural background.

Risk attitude manifests in three ways; the two extremes being risk–averseness, where individuals are more inclined to avoid risk, and risk–aggressiveness (risk seeking), where individuals are actively seeking to take risk. Between the two extremes, there are individuals who are neither actively seeking risk nor seeking to avoid risk.

As mentioned above, risk attitude is influenced by perceptions, which could have been formed overtime– right from one’s family background.

Generally speaking, individuals who come from strict families that follow a rule–based approach, tend to be risk–averse, because they have high regard for conformity to the rules and/or standards.
On the other hand, individuals from open families tend to be risk aggressive, willing to explore every opportunity with little regard to standards, policies, procedures, and sometimes even laws and regulations.

This of course is a generalization, there are always exceptions to the rule.

From the organizational point of view, the two types of individuals are equally important because, whereas the risk–aggressive individuals are able to exploit opportunities and create value for the organization, the risk averse individuals provide critical checks and balance mechanism against potential recklessness and overzealousness of the risk–takers, which can erode the value of the organization. The risk averse individuals provide a defensive mechanism while the risk takers provide an offensive mechanism.

In conclusion, understanding risk from a narrow view of “danger” limits the organization from taking advantage of opportunities that create value for the organization, while overzealousness in pursuit of a certain objectives can create a disaster for the organization. Therefore, striking an appropriate balance is the key to success.

Joshua Kibirige,
Anti–Money Laundering Manager,
National Social Security Fund

The Future of Pension Funds in the Face of Declining Interest Rates on Bonds

Pension funds, are by nature risk–averse and therefore prefer investing most of their funds in government securities (bonds.) But with a steady decline in global interest rates on bonds, where does that leave them?

Investment is usually guided by the organization's risk appetite. Some organizations are more willing to invest in high risk ventures because of the high anticipated returns, while others such as pension funds, are by nature risk–averse. Pension funds prefer investing most of their funds in government securities (bonds)– See figure 1 and figure 2 below).

Fig. 1: Asset allocation for selected OECD Countries

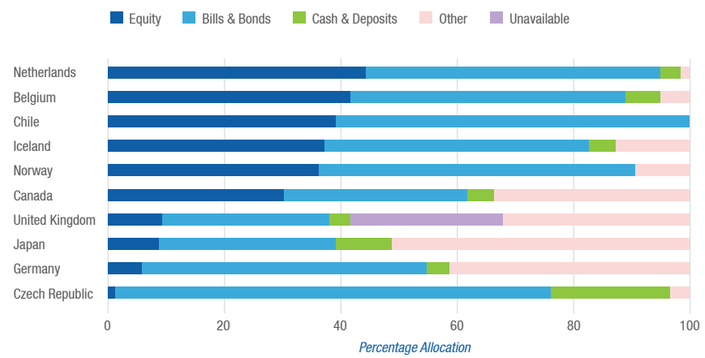
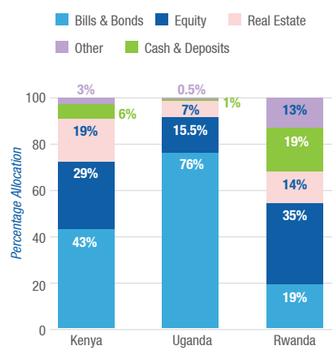


Fig. 2: Asset allocation for selected pension funds in East African countries



According to Alexander Marinon's article in the PRIMA (Professional Risk Managers Association) magazine, this ensured that savers' projections with regards to post–retirement income would be met. However, over the years there has been a steady decline in interest rates on bonds globally. For example, according to Alexander, prior 2008, the 10–year German government bond was yielding around 4.0%. However, in 2019, twelve years later, the same 10–year German government bond was yielding –0.2%.

Fig. 3: 10–year Government Bond yields for selected OECD Countries

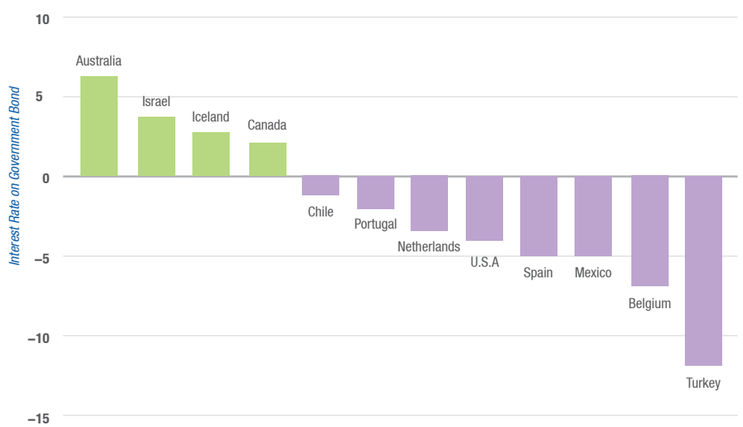
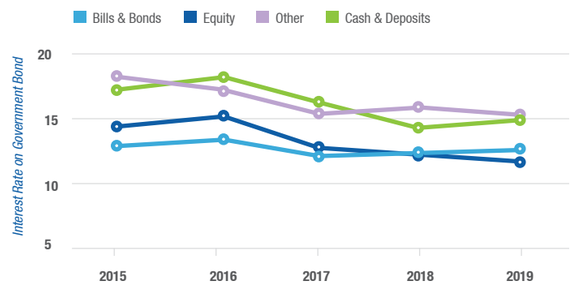


Fig. 4: Average interest rates on bonds in East Africa for the last five years



Germany is not alone, the situation in other EU countries like France and Netherlands is not any different. In Greece, the 10–year bond yields 1.36%, while the Italian bonds of a similar maturity yields a paltry 1.18%.

Whereas the yield on the government bonds in Uganda and in other East African countries are still relatively high, as the economies expand, especially due to oil exploitation, the governments are likely to reduce their demand for domestic borrowing, which will force the yields on government bonds to significantly go down.

According Fitch, a research company, there are close to $10 trillion outstanding government bonds that yield negative rates globally, of which close to two–thirds belong to Japan.
The remaining ones are located in Europe – see figure 3, where the ECB and several Scandinavian countries have been forced to keep rates at record low levels.

Pension funds face a serious dilemma; they need to tread carefully to avoid losing pensioners' savings in risky investments on one hand, on the other hand, the returns on the risk–free investment are dwindling, implying that they may not have adequate savings to cover their obligations to their members.

According to Alexander, in Germany for instance, major pension fund schemes are facing a real dilemma, most of them are not allowed to invest more than 35% in risky assets.

Inevitably pension funds may be forced to invest more in risk assets so as to generate reasonable returns to cover their obligations for their members' retirement.

However, such investments as real estate, cannot be easily liquidated to meet immediate cash needs. Others such as equity, are highly volatile; they can generate high returns but they can also generate significant losses.

In his article in the PRMIA January 2020, Alexander Marinon writes that in Japan, which has for years suffered from low yields, funds have started to invest more actively abroad. A prime example is Japan's Government Pension Investment Fund (GPIF), which announced that it would allocate 5% of its €1.25 trillion assets into alternative assets.

It has even dropped its government bond holdings from 60% to 35% during a five–year plan, which was in the making since 2014. Still, change is slow and troublesome. As an example, two of the largest US pension funds have allocated close to 29% of their portfolios to such alternative investments – a mix of real estate and private equity.

In conclusion, this presents a real dilemma for pension funds in the future, because their cash cow has always been sovereign bonds, which are low–risk assets. However, as explained above, the returns on these investments are getting low and low globally. Pension funds will be forced to adopt alternative investments, which are generally considered highly risky. Having no option but to undertake alternative investment, pension funds will need to develop a robust and agile risk management framework to enable them to take advantage of opportunities such as private equity, real estate, agriculture, etc, as well as effectively controlling the downside.

According Fitch, a research company, there are close to $10 trillion outstanding government bonds that yield negative rates globally

Adolf Kaija Baguma
Operational Risk Manager,
National Social Security Fund

Understanding Fraud Dynamics

Nearly every organization, large, medium or small, not–for–profit or for profit, has experienced fraud at some point in time.

For the few organizations that might not have experienced fraud, it is just a matter of time, or else, fraud could have taken place but the incident has not been detected– no one is immune from fraud.

But what is fraud?

A lot has been written and will continue to be written about fraud, for as long as it remains a menace in our midst.

According to Merriam webster dictionary of law (1996), fraud is any act, expression, omission, or concealment calculated to deceive another to his or her disadvantage, specifically, a misrepresentation or concealment with reference to some fact material to a transaction that is made with knowledge of its falsity, and/or in reckless disregard of its truth or falsity and worth the intent to deceive another and that is reasonably relied on by the other who is injured.

As stated above, every organization has been hit by fraud at a certain point in time. In a recent survey by PwC, named "Global Economic Crime & Fraud Survey 2020, 47% of the 5,000 respondent companies in 99 territories admitted having experienced fraud in the last 24 months. The financial loss was staggering– USD 42bn! Interestingly, only 56% of the affected companies conducted investigations into their worst fraud incidents

The dilemma is that some organizations are not comfortable disclosing a fraud incident for fear of ruining their image. Such organizations believe that if they disclose that they have been hit by fraud, then the public will lose confidence in their systems and consequently they lose competitiveness.

None–disclosure also means that the affected institution is reluctant to take punitive measures against the fraudster, e.g. pursuing criminal charges against him/her.

This partly contributes to the escalation of fraud incidents, as the fraudsters do not see real danger associated with committing fraud.

Additionally, the laws in Uganda and in many other jurisdictions, which presume one is innocent until is proved guilty, also make it difficult to successfully prosecute the fraudsters, because the fraudster usually ensures that it is extremely difficult to trace any audit trail of a fraudulent transaction.

Consequently, billions of money are lost every year, and the impact on organizations is often times enormous. In some cases, it has led to the collapse of the affected institutions.

Although organizations have taken efforts to detect and prevent fraud, the vice persists and continues to daunt many organizations. The efforts against fraud do not seem to be yielding the desired results.

Interestingly, in majority cases, a fraud incident involves an internal party– the employee. Every survey, study and comparison across segments has shown repeatedly that those individuals who steal from a business, the most are employees.

Part of the reasons why fraud continues unabated could be that those who are trying to fight fraud have not appreciated the key ingredients of fraud– the environment that enable fraud to flourish. These according to COSO [Committee of Sponsoring Organizations], are three, that is; Opportunity, Pressure and rationalization, which are like three pillars or corners of a triangle, hence, the "fraud triangle"

Opportunity

Fraud opportunity refers to the circumstances or the environment that makes it possible for fraud to take place.

These include but not limited to:

i. Ineffective internal controls.
Internal controls are the policies, procedures, guidelines that are put in place to ensure integrity of transactions, efficiency and effectiveness of operations.

Weakness in internal control include lack of or poor segregation of duties, ineffective supervision, undocumented procedures, lack of audit trails for transactions etc.

A typical case of breach in controls happened in one of the organizations where I worked. A graduate accountant trainee was allowed to manage arious stages of the payment process single–handedly. She would write cheques and present them for signatures, withdraw funds and appropriate it.

Within a short period of time, she started forging the cheques by inserting additional figures to change the approved amounts. For instance, if a cheque was written as;

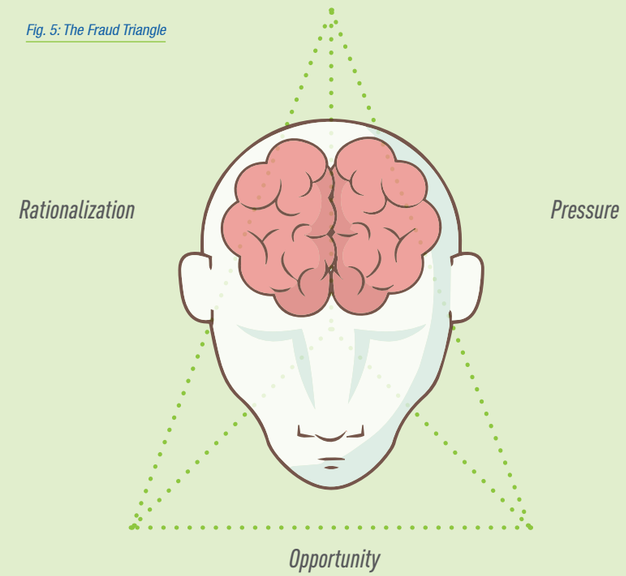
Amount in figures: [200,000]
Amount in words: [Two hundred thousand only]

She would change it to:

Amount in figures: [2,200,000]
Amount in words: [Two million two hundred thousand only].

Following a forensic audit, it was discovered that the company had lost over UGX 300M within a short time.

Fig. 5: The Fraud Triangle



ii. Inappropriate tone at the top
Culture of an organization is shaped mainly by the manner and style of management/board.

If the leaders (board & executives) behave in an unethical manner, this will reinforce the fraudster's rationalization of fraud.

Management need to send a strong signal against fraud, by putting place strong internal controls and severely punishing those who commit or attempt to commit fraud.

iii. Lack of or unreliable accounting policies
Accounting governs how items are recorded in the books of accounts and financial statements. If the organization lacks accounting policies or if they are vague or inconsistent, this will give the staff the opportunity to commit fraud.

Pressure

A number of people are driven into committing fraud by either real or perceived pressure. Real pressure could be because of financial distress, where an individual is highly indebted and his income cannot settle his obligations. The perceived pressure could arise out one comparing him/herself with others whom he/she considers to be well off. The other source of pressure could be because of the individual's lifestyle. If the individual wants to maintain an expensive life style, this will put pressure on him/her to get money at any cost.

Rationalization

The other factor that completes the fraud equation is rationalization of fraud. Having identified the opportunity and pressurized enough, the individual begins to create justifications for committing fraud. Statements like, "After all I am paid peanut here", "No one will find out", "I am not the first one to do it", "I am taking only 2million, it won't make the organization collapse." etc. begin to form in the individual's mind.

In the case of Jessica Harper, who was the Head of fraud and security for digital banking at Lloyds, she tried to justify her fraud actions, amounting to £ 2.4M, committed between 2007 and 2011, by stating that: "I saw the opportunity and thought: 'Given the hours I work, I deserve it'. "If I went to work for another company, I would probably be earning four times as much."

A combination of the three pillars of the triangle result in fraud. It is important to note that, among the three pillars, it is only the Opportunity that the organization has direct control over. By removing the fraud opportunity, e.g. strengthening internal control, setting the appropriate tone at the top, having proper accounting policies and procedures, inter alia, the organization can significantly minimize chances of fraud.

Indirectly, the organization can also ensure that it creates a work environment that does not exert excessive pressure on the employees, e.g. poor remuneration, working overtime– until late in the night, etc.

Deterrence

In addition, organizations can institute a number of other interventions to minimize fraud as discussed below;

Whistleblowing
This can be an effective fraud deterrent tool, where an organization has established a conducive environment where whistle blowers feel protected from vengeance.

Segregation of duties
Key tasks within each key job processes should be segregated such that no single person can authorize, initiate and execute a transaction single–handedly.

Job rotation/ Leave
Job rotation and mandatory leave policies are best practices that can help to prevent employee fraud.

Both of these practices discourage fraud and other abuses because employees know that another person will be assuming their duties and the new person could discover certain patterns of behavior. These should not be taken merely as other human resources practices but as effective tools in fraud mitigation.

Training and sensitiization/ integrity campaign
There should effective fraud awareness programmes in place, and effectively communicated to all employees. In addition, periodic fraud awareness training for all employees should be conducted.

Edward Senyonjo
Head of Risk
National Social Security Fund

Risk Hedging with Forward Contracts

A hedge is an instrument to reduce the risk of price movement in an asset. Normally a hedge consists of taking an offsetting position in a related security such as futures contracts, forward contracts, options, swaps, etc.

This article, however, focuses on hedging with forward contracts, which is the simplest form of hedging.

Hedging is similar to insurance because if you have taken a hedge against a loss and the loss crystalizes, you are compensated, but hedging is not identical to insurance because in some cases, you do not pay a premium to acquire a hedge– for instance, using a forward contract to hedge an exposure does not require any payment.

Secondly, insurance shifts the risk of loss from the insured to the insurer, while hedging simply reduces or offsets the hedger's risk.

Historical perspective

According to an article by Federico Stiegwardt, hedging dates as far back as the mid–1800s, although some accounts point to the fact that hedging existed even earlier than that. In the mid–1800s, Chicago was a commercial centre of the USA, where farmers and traders converged to conduct trade. Farmers were selling grain to buyers who would ship their grain all over the US. More often than not, a number of dealers would then offer a price to secure those purchases for a limited amount of grain. However, the supply of grain far exceeded what the dealers would buy. That meant a lot of grains would go to waste and the farmers made losses.

Over time, farmers and dealers came up with an idea, where the dealers were required to make a commitment to buy the grain in the future at a price agreed today, while the farmers were required to make a commitment to deliver the grain at a specified period. This commitment would be written on the blackboard, and would be binding on both parties– for the farmer to deliver the grain and for the dealer to pay for the grain at the agreed–upon price. These commitments created price stability and enabled the farmers to plan the production, while the dealers were able to manage their cash flows better.

Hedging in the contemporary world.

As more and more farmers and traders joined this trading arrangement, this led to the introduction of the Chicago Board of Trade in 1848 to regulate the "commitments".

From then on, the concept of commitment evolved into the modern day concept of hedging that has led to the development of large exchanges worldwide, with the Chicago Mercantile Group (CME), being the global leader as a derivatives market. As mentioned above, there are many derivatives that can be used for hedging, however, the focus of this article is on hedging with forward contracts, specifically currency forwards.

Forward contracts

A forward contract is an agreement between the seller and the buyer of an asset at an agreed price applicable in the future. The price is agreed now, but the exchange takes place at an agreed price in the future. The seller has an obligation to deliver the asset at the agreed price, date and location, and the buyer has an obligation to pay for the asset.

A forward contract is traded in the over–the–counter market, usually between two parties, i.e, between two financial institutions or between a financial institution and one of its customers. The one who agrees to sell is said to have a short position, while the buyer is said to have long position.

This obviously creates a credit risk to the parties. The financial institutions, however, minimize this risk with a spread between the bid rate and the offer rate [in case of a currency forward contract]–see a hypothetical example below.
The bid rate is the rate at which the bank is willing to buy the underlying asset, and the offer rate is the rate at which the bank is willing to sell the underlying asset.

The most popular form of forward contracts are currency forward contracts; this is where two parties agree to exchange currencies at a future date at a rate agreed upon in advance. Regardless of what the spot rate is at the time of exchange, the applicable exchange rate will be the rate that was agreed in the forward contract.

Advantages of forwards

i. Forwards are based on mutual understanding/agreement of parties, and they can be written for any amount
ii. They usually [but not always] offer a complete hedge
iii. Unlike options, they do not require any payment to initiate them
iv. Unlike swaps, futures, and other derivatives, forwards are simple– easy to understand

Disadvantages of forwards

i. Forward contracts create credit risk for the parties involved.
ii. It may be difficult to find a counter party
iii. Just like any other binding agreement, it may be difficult to cancel a forward contract.

In conclusion, it is important to note that hedging offers a very good strategy for mitigating the risk of loss arising from changes in the price of the underlying asset. But the hedger needs to be aware of the fact that prices could go against the hedge. Therefore, the hedger needs have good knowledge of the price movement of the asset to be able to make the right prediction.

How a Currency Forward Contract Works

Suppose on the 04/03/2020, a Ugandan importer expects to pay USD 300,000 worth of imports in the next three months and is worried that the dollar might appreciate against the shilling by June 2020 (three–month time).

He can hedge the foreign exchange risk by agreeing to buy a dollar at UGX 3,700 per dollar, i.e, 3–month forward– see table 1 below. Which means that he will pay UGX 1,110,000,000 [300,000 X 3,700] to obtain USD 300,000 that he needs to clear the goods.

Assume that the spot exchange rate on 04–06–2020, when the exchange takes place, is 3,705. That means that by buying each dollar at 3,700 instead of 3,705, he has eliminated the loss of UGX 1,500,000 [(3,705 – 3,700) X 300,000].

However, it is also possible that the exchange rate could fall to 3,695; in which case the importer would lose UGX 1,500,000 [(3,695 – 3,700) X 300,000].

This is because the importer is obligated to buy each dollar at 3,700, regardless of the spot rate at the time of exchange.

If K and St are the delivery (forward) price and spot price of the asset at maturity of the forward contract respectively, payoffs from a long and a short position are as follows:

Payoff [Long position– Buyer] = St – K
Payoff [Short position– Seller] = K – St

It is important to note that much as hedging offers great benefit to the hedgers in terms of minimizing the risk of loss arising from price movements, it can also expose the company to potential loss if the price movement is against the hedge as explained above.

Table 1: Forward quotes for the USD /UGX exchange rate on 04/03/2020.

	Bid rate	Offer rate
1–month forward	3,685	3,695
2–month forward	3,687	3,697
3–month forward	3,690	3,700

USD = US dollar, UGX = Uganda shilling

Ian Mugisha
Risk Management Officer – ERM,
Uganda National Roads Authority.

Risk Management -A tool for Performance Management

Achievement of organisational objectives is greatly influenced by how well risk and performance are managed.

Therefore, aligning risk management practices to organizational performance improves the execution of organisational strategy.

According to Carla Ruder (2016), "it wasn't too long ago that risk was a taboo four–letter word among business leaders–something that needed to be avoided at all costs". But today many organizations consider risk an integral part of business, which needs to be managed so as to achieve organizational goals. Carla reiterates the need for business executives to understand and think strategically about known and emerging risks that affect or are created by business strategy decisions.

In this article, an attempt is made to show how risk management can be used as a tool for enhancing organizational performance, by exploring the relationship between risk and performance management, and identifying ways through which risk management can support organizational performance.

Firstly, every entity, private or public, exists to create value for its stakeholders, that is, profits/dividends for shareholders, products for customers and environmental sustainability for the wider public.

These values are communicated through a strategy in form of SMART [Specific–Measurable–Attainable–Realistic– Timely] objectives, with specific targets.

Secondly, the organization puts in place mechanism to execute the strategy and evaluate the extent to which it attains its strategic objectives, through performance management systems. However, at planning stage a organization will never be sure that all the objectives or which objective it has set will be achieved, due to uncertainty/risk [ISO 31000– "Risk is the effect on uncertainty on an objective, whether positive or negative]. The role of performance management, therefore, is to ensure that the negative effects are minimized and the positive effects are enhanced.

This calls for establishment of performance indicators that are both forward–looking (leading) and backward–looking (lagging). Unfortunately majority of organizations concentrate on lagging indicators, which provide information relating to past performance, as opposed to the future. Such lagging indicators include "Number of units produced per hour", "Number of defects per batch", etc.

On the other hand, leading/predictive indicators provide information on what is likely to hinder progress or enhance success before any problem is encountered.

It wasn't too long ago that risk was a taboo four–letter word among business leaders–something that needed to be avoided at all costs. But today many organizations consider risk an integral part of business.

This is when risk management comes in handy to enhance performance. Risk indicators provide management with an early–warning mechanism for performance shortfalls, which can be addressed before things get out of hand. For example, if the organization's objective is to increase productivity, one of the factors (risk) that can hinder it from achieving this objective would be "Loss of key staff", and one of the causes of loss of staff (Risk Indicator) could be "Low pay". Therefore, analysing the organization's pay scale in relation to the industry/market, can provide early–warning signal of staff turnover, which affects productivity.

According to J Raid and S Estonia (2012), separating risk management from performance management shifts the responsibility of risk management from business operations and hence may expose the entity to underutilisation of resources and missed opportunities.

Suffice to say, therefore, risk management should be embedded in the day–to–day activities of an organisation in order to ensure effective alignment of business processes to risk management.

Furthermore, for an organisation to fully enjoy the benefits of risk management as a tool for performance, risk management metrics must be adopted in a performance measurement tool such as the performance–balanced scorecard (BSC)– "What gets to be measured, gets to be done". In the case of the BSC, performance is aligned to four perspectives; financial, customer, processes and learning and growth. Implementing such a scorecard would require for example analysis of potential financial risks and assigning actions and action owners. These action owners would be evaluated in a performance cycle to assess the implementation of the actions and effectiveness.

There is no doubt that where the actions are effective and have been fully implemented, it would positively reflect on the performance and vice versa.

According to Smart and Creelman (2003), Risk Based–Performance Management provides organizations with an integrated strategy and a risk management approach that places risk, and specifically risk appetite, at the core of strategy execution. In this sense, risk management enhances monitoring business targets as leading indicators using risk appetite. The risk appetite is simply a measure of how much risk an entity is willing to take to achieve the desired objective. This provides an upper or lower limit within which the operations of the entity are executed in order to maximise resource utilisation.

In my view, best risk management practices increase the chances of implementation of the objectives of a strategy, because it studies the effect of uncertainties that may affect the strategy in form of risk and reward. Thereby, supporting the organisation to have a better performance efficacy, since aligning it to objectives is as good as directly aligning it to strategy.

In conclusion, both performance management and risk management focus on ensuring the organisation's objectives are met. However, while managing risk may result in the achievement of objectives (resulting in a great performance), performance management does not necessarily guarantee a healthy risk environment. Therefore, every leader should embrace risk management as a tool for fully utilising opportunities and or resources which in turn support realisation of organisational strategy and objectives.

Jesse Okutre
Investment Risk Analyst,
National Social Security Fund

COVID-19: An Effective Crisis Management Plan can make a Difference.

As at March 23 2020, there were 307,000 confirmed coronavirus infections and 13,049 deaths (cumulative) globally, with the epicenter in Italy, with a staggering death toll of 4,825, which was the highest in the world higher than the highest recorded in China (3,261) by 1,564 deaths [https://www.worldometers.info/coronavirus/]

The coronavirus was code named COVID–19 by WHO on February11, 2020. The disease outbreak was first realized in Wuhan in China and was reported to WHO on December 31, 2020. Wuhan, which was a bustling commercial city, turned into a ghost city, as people were directed to stay home, while the authorities took drastic measures to avert the spread of the virus. COVID–19 soon spread across the globe, as Chinese and other nationals, who have been infected travelled to other countries.

Cases of COVID–19 began to be reported in other Asian countries such as Taiwan, Singapore, South Korea, Iran, etc. In Europe, countries such as Italy, Spain, Germany, France, etc, were affected. The USA, Brazil, Canada, etc, and a number of African countries also confirmed cases of COVID–19.

How China dealt with the crisis
China was credited for tackling the pandemic head–on. China's strategic intervention included locking down Wuhan city, construction of two makeshift hospitals with a total bed capacity of 2,300 in unprecedented time– 10 days!

According to Sean Fleming's article of March 11, 2020 on the World Economic Forum website– www.weforum.org, on January 23, 2020, Wuhan and other 15 cities in Hubei province were placed under strict quarantine after the area was affected by coronavirus infections.

The lockdown affected nearly 50 million people. Medical and healthcare workers were brought in from all over China to help. Public transport was paralyzed, as railways, flights, and the metro systems in Wuhan were closed. People in Wuhan were directed to stay at home. To leave Wuhan, you needed permission from the authorities. All shopping malls, offices, restaurants, supermarkets, schools, factories, etc, were ordered to close.

However, despite all these measurements, the number of infections and death kept rising, until March 22, 2020, when China did not report any new infection for the previous four days.

As I wrote this article, China had the lowest infection rate of COVID–19. The patients that had recovered from the disease had been discharged from hospitals, and people across China were beginning to go back to work.

A case of excellent crisis management.
The most amazing example of effective crisis management was by Singapore and Taiwan. For example, the first case of COVID–19 in Italy was confirmed 10 days after Taiwan, but by March 21,2020, Italy had more than 47,000 cases and 4,032 deaths, while Taiwan had only 153 cases and 2 deaths, despite being closer to China than Italy.

Taiwan's and Singapore's effective COVID–19 crisis management could have been informed by their experience with SARS (severe acute respiratory syndrome) in 2003. According to an article by Adam Rogers, on wired.com, after SARS (2003) and H1N1 (2009), Singapore built a robust system for tracking and containing epidemics. As soon as the genetic sequence for the new COVID–19 were published, Singapore developed their own test kits and increased produvction of the materials required for those test kits. This sharply contrasts with USA, which did not have enough test kits for nationwide use at the onset of the COVID–19 outbreak in USA.

The most amazing example of effective crisis management was by Singapore and Taiwan. For example, the first case of COVID–19 in Italy was confirmed 10 days after Taiwan, but by March 21,2020, Italy had more than 47,000 cases and 4,032 deaths, while Taiwan had only 153 cases and 2 deaths, despite being closer to China than Italy.

In the article; "How Taiwan and Singapore managed to contain COVID–19, while letting normal life go on", Tom Blackwell writes that Singapore managed to avoid the kind of mass social disruption that became a common phenomenon in most countries that got affected by the COVID–19. In Singapore and Taiwan, schools, workplaces, stores, and restaurants, all remained open. Both Singapore and Taiwan conducted mass testing and instituted strict measures for isolating people who had or were suspected to have COVID–19, tightly controlling international travel and tirelessly pursuing those who had contact with the infected.

According to the article, Singapore deployed police to track contacts and constantly monitored those under quarantine. Taiwan, according to the article, merged citizens' recent international travel history with their digital health–insurance files and let doctors and pharmacists access it all, while levying stiff fines for quarantine violations. Students took steps to avoid crowding by undertaking on–line learning.
Unlike many other countries that were affected by COVID–19, Singapore took COVID–19 very seriously from the start, and was therefore, able to put the outbreak under control.

Many countries, particularly in the West, dragged their feet in taking appropriate measures to combat COVID–19. According to The Guardian, after weeks of government inaction in the face of the growing crisis, countries such as Spain, France, Germany, UK and the US, began to take drastic measures which would have been taken at the onset, such as lockdowns and approving billions for rescue plans.
If they had taken such measures in a timely manner, they would have avoided the calamity that unfolded. Taiwan, Hong Kong and Singapore, which were affected much earlier than Europe, acted swiftly and were able to control the spread of the virus; they have registered only a few deaths and a had a few cases.

Key lessons learnt
i. Always be prepared and do not underrate any crisis.
ii. Formulate different crisis scenarios and test your crisis management plan before the crisis hits
iii. In a crisis, quick decision–making is critical. Procrastination simply escalates the problem and increases collateral damage.
iv. Extraordinary situations require extraordinary actions. Do not be bogged down with bureaucratic red tape during a crisis.

Conclusion.
Although no one ever anticipated that a disease such as COVID–19 could erupt around this time and bring the world to its knees, including the world's most technologically advanced and economically powerful nations, the well prepared, most agile and less bureaucratic nations like Singapore and Taiwan, were able to bring the virus under control.

Dr. Paul Kasenene
Managing Director,
Wellcare Ltd

Our Health is a Function of our Choices

The coronavirus pandemic that the world is experiencing, has really highlighted how important life is.

It has shown us that no one wants to be sick, everyone wants to be well and stay well and that disease is probably the biggest threat to humanity.

Although all the attention and focus globally and locally is now on coronavirus, the reality is, there are many other diseases that affect humanity. More than ever before, more and more people no longer feel as well as they would like, due to illness. They are struggling with various challenges to health, experiencing a decrease in health and vitality.

The threat to our health and wellness

Many of us are struggling with fatigue, low energy, headaches, poor memory, low mood, low sex drive, back pain, poor sleep, bloating, rapid weight gain, especially around our waistlines, etc. We also have an epidemic of lifestyle diseases (also called non–communicable diseases) like diabetes, high blood pressure, heart disease, cancer, asthma, arthritis, obesity, among others.

Some of us cannot even climb a few stairs or run a few meters without being breathless. But why is this the case?

Important facts about health and wellness

Many of the health problems we experience today were non–existent many years ago. Before independence in Uganda, diseases like diabetes were only read about in text books.

Anyone can experience these health problems, including those with seemingly lean stature, and the children, if they do not mind about what they eat (or not eat) and/or what they do (or not do). Unlike cars or other equipment, the body has no spare parts; nither money nor medical insurance can buy health or wellness.

However, the goods news that, all these health or wellness challenges can be prevented.

Choose to be healthy

It is every living thing's desire to be healthy and well at all times. However, it is interesting to note that our actions or inactions are often times not in tandem with this universal desire of every human being– being health and well. What we eat and lack of exercise for example, determine whether we develop diabetes, high blood pressure, heart disease, cancer, obesity, etc. So, it all boils down to the choices we make!

The determinants of our health status are not our genes, health care, hospitals, or doctors, but the choices we make everyday about what to eat and not eat, and what to do and not to do.

In fact, doctors often treat symptoms and not necessarily the causes of the disease. When someone has diabetes, rather than treat the symptoms of the disease (which is high blood sugar) with drugs, we should understand the cause of diabetes (which is usually diet and lifestyle), and manage that. Again it is about choices– are you willing to change your diet and/or life style to address the causes of diseases? What choices are you making today? Are you choosing health or disease?

Below are some of the right choices you can make to remain health:

1. Stay hydrated.
All the cells in our body need adequate water to function well. Not having enough water in our body system can lead to malfunction or dysfunction of cells. We should all drink at least 2 litres of water each day, although the optimal amount of water needed by your body is computed by diving your weight (Kg) by 30. E.g if you weigh 75Kg, should drink 2.5 liters [75/30 = 2.5] of water daily. Remember to drink throughout the day, not all at once.

2. Eat better.
Going through this requires a book of its own; fortunately, I have written one called "Eat Your Way to Wellness'. Make sure to get yourself a copy. However, here a few important things to consider about eating right:

i. A minimum of 90% of our food should come from plants —no more than 10% from animal foods.

ii. A minimum of 90% of our food should be natural, whole, unprocessed, unrefined and not modified like GMOs.

iii. 50% of our diet should be fruit and vegetables, and 50% of our food ideally should be uncooked.

Consider the following guidance on how often to eat particular foods:

a) Eat these foods in abudance

i. Cruciferous vegetable [Cabbage, Sukuma wiki, broccoli, cauliflower, carrots, beetroots, etc
ii. Fruits
iii. Immune–boosting foods [garlic, onion, lurmeric, ginger, mashooms
iv. Nuts, chia, flax, pumpkin & sesame seeds, almond, cashew, ovaccado

b) Eat these foods in moderation
Animal fats [not >300 gm per week], food rich in carbohydrates [Oats, maize, sweet potatoes, pumpkins, yam, matooke, cassava]

c) Foods to avoid
Sugar, sugary drinks [soda, packet juice, etc], sugary foods [sweets, lollipos, biscuits, ice cream, etc], deep fried foods.

Food rich in refined carbohydrates and foods made from refined wheat like white bread, chapati, cake, mandazi, pasta, and biscuits as well as other foods made from refined grains including white rice, cornflakes and refined posho.

Deep–fried foods such as chips, crisps, fried chicken and other such foods. Deep frying is linked to cancer and heart disease and processed meat like sausages bacon, ham and frankfurters.

3. Keep active
Being active helps keep your immune system strong. Aim to get at least 2 to 3 hours a week of moderate exercise –the more, the better. Exercise doesn't have to be at a gym or at a special class. Anything that gets your heart rate up and makes you sweat, will count –even walking, dancing, or playing sports with friends.

4. Get enough sleep.
Sleep is the silent factor in our quest for great health. It is the time that the body uses to heal, detoxify, regenerate and restore our bodies. It is very essential if you want to remain healthy. The body requires at least 7 hours of sleep each day, 6 hours should be the minimum. It is best to go to bed early (not later than 9.00PM), and rise early.

I hope we can all begin to rethink the choices we make every day and how small things we do can make a big impact on our health. The good news is that we can all make better choices if we decide to. They may not always be the easiest, but they will ultimately be worthwhile.

Remember, many people will eventually have to give up their work and sell their wealth to try and get back their health. Let that not be your story. Be smart, make healthy choices today.

Michael Sendiwala
Investment Risk Manager
National Social Security Fund

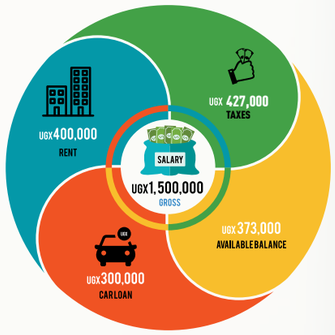
The Corporate Lifestyle Dilemma.

For those of you who work or have worked in the corporate world will agree with me that corporate organizations often times try to project an image of class.

This is manifested in various was ways; the interior and exterior design of the offices, the furniture, air–conditioning, the cars, to mention but a few. This also affects the lifestyles of employees of these organizations.

Employees are supposed to dress and behavour in a way that projects the same image; for instance, many corporate entities have a well–defined dress code, and they expect the employees to be smartly dressed at all times.

Illustration



Maintenance of a high class standard creates an expensive lifestyle for the employees, and this drives a number of them to financial indiscipline such as committing fraud.
Often times we have had a story of a young graduate who gets a job which pays him, for instance, UGX1, 500,000– gross, with a take–home of UGX1,073,000, he lives in an apartment where he pays UGX400, 000 and obtains a car loan for a monthly installment of UGX300,000. So, when he pays the loan installment and rent, he remains with UGX 373,000 which can barely meet the monthly car maintenance costs, not to mention the expenditure on food and other personal expenses.

It is likely that he will begin to default on the loan repayment. Faced with this dilemma, he asks for a salary advance, which may not be enough to address his troubles. The next move is to run to a money lender for a quick cash bail out to repay the car loan. Although the money lenders provide quick cash, the interest rates are usually so high, ranging between 50–150% per annum. The employee is now in a deep financial crisis, and he has to think of a way out.

This is the starting point of committing fraud– the financial pressure. The employee now starts to look for a way to obtain money fraudulently from his employer.

Many employers are losing their good employees because of financial pressures emanating from financial indiscipline, and the solutions seem tricky because of the grey area around privacy (to what extent can the employer inquire about the employee's financial status?).

With too many societal demands and a number of unscrupulous lenders, willing to provide credit within seconds but expensively, employees are always willing to take these options without considering or questioning the medium – long term impact of the financing source on their future cash flows.

The other trend that is emerging is where corporate employees try to save and invest in small business/start–ups so as to supplement their income from employment. Usually the first option is agriculture.

This is because it is assumed, though wrongly, that agriculture is simple– does not require sophisticated techniques. The idea of investment per se is a good thing, however, a number of these start–ups have not lived to see their first birth day.

The reasons for this are many, but two of them being that due to their busy schedule, a number of corporate employees don't have time to monitor their businesses and take timely decisions. Usually they visit their business premises once in week (Saturday/Sunday), or once in a month.
This makes the businesses more vulnerable to mismanagement and fraud. A start–up is like a baby, extremely fragile; it requires the attention of the mother (owner) at all times.

Corporate employees who are too business to monitor their business would rather invest in government securities, which do not require the same level of monitoring as start–up businesses.

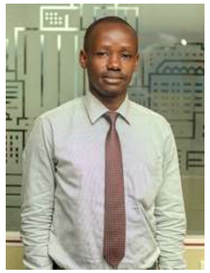
The other reason for failure of the investment, perhaps the most important one, is wrong investment decisions, especially investing without a clear goal.

Maintenance of a high class standard creates an expensive lifestyle for the employees, and this drives a number of them to financial indiscipline such as committing fraud.

A proper investment process begins with a clear investment goal and specific time horizon (Short term, medium term and long term). Most corporate employees focus on attaining their aspirations (dream houses, cars, etc), before breaking even, and when their obligations and needs kick in, a crisis ensues, as they hop from one money lender to another. Some wrongly invest all their resources in highly risky ventures, hoping to become rich overnight, and when the investment goes bad, all the capital and interest is wiped.

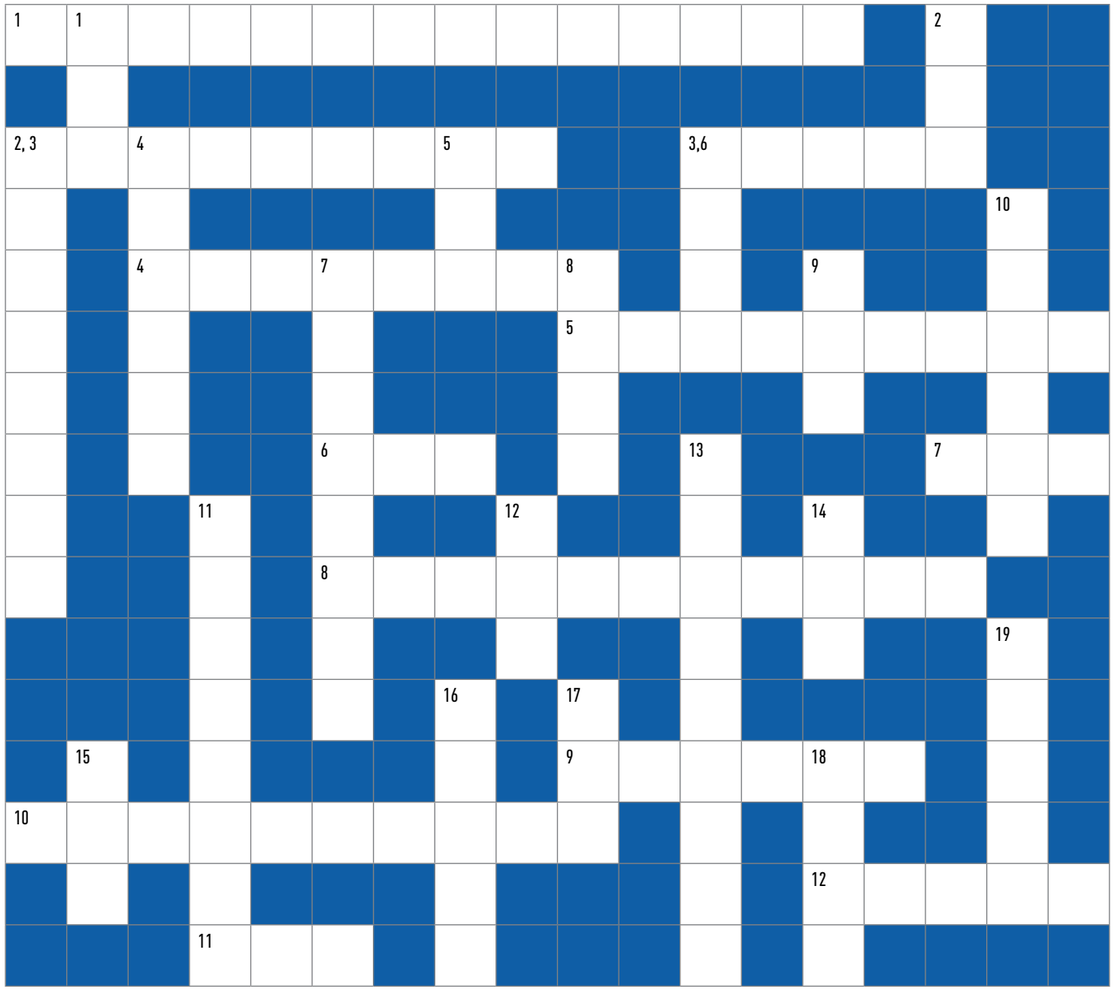
Consequently, the employee is pushed into a crisis, which deepens with borrowing as explained above, and the temptation to commit fraud kicks in.

In conclusion, corporate employees need to learn to manage their lifestyles in line with their incomes. It is suicidal to live an expensive lifestyle which denies you the opportunity to save and invest. Sooner or later, the job could be no more and you drift in poverty.



Robert Masiga
Operational Risk Officer,
National Social Security Fund

Test Your Risk Knowledge



Across

1. A step in the risk management process,(14)
2. The risk that results from adverse business decisions or improper implementation of decisions or lack of responsiveness to industry changes,(9)
3. The risk as a result of non–compliance with say the statutory requirements,(5)
4. Seriously disrupts the functioning of an organisation,(8)
5. Method used to identify risks by use of questionaires,(9)
6. A framework for managing risk at organisation level,(Abbr.3)
7. The means of systematically assessing the potential impacts resulting from unavailability of a service/product as a result of a disruptive incident,abbr.(3)
8. A practice where laundered funds are made to appear as legitimate,(11)
9. Model used to analyze bank risk condition,(Abbr.6)
10. Risk identification technique that encourages everyone to be free and openly participate,(10)
11. The integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity, (Abbr. 3)
12. Can be used to mean indicators of risk,(5)

Down

1. An examination of each step in a disaster recovery plan as outlined in an organization's business continuity, (Abbr.3)
2. A collection of permissions granted to the users to ensure confidentiality, (Abbr.3)
3. The risk that cannot be diversified,(8)
4. A risk treatment method involving decisions to put measures in place to moderate the impact of occurrence of identified risk,(6)
5. Area where there are high cyber incident attacks in the world, (Abbr.3)
6. That has been taken away or cannot be recovered say after disaster,(4)
7. The amount and type of risk that an organisation can take on in pursuit of its strategic objective,(8)
8. The effect of uncertainty on an objective. (4)
9. A global profession for those who manage risk, (Abbr.3)
10. The risk of the possibility of a loss resulting from a borrower's failure to repay a loan or meet contractual obligations,(6)
11. A stage in money laundering involving use of multiple accounts, banks, intermediaries, corporations, trusts, countries to disguise the origin,(8)
12. Individual with a high profile political role, or who has been entrusted with a prominent public function susceptible of money laundering, (Abbr.3)
13. A practice in money laundering where illegal funds or assets are first brought into the financial system,(9)
14. A semi–autonomous body established by the Anti–Money Laundering act, 2013,(Abbr.3)
15. Is a facility an organization can use to recover and restore its technology infrastructure,(Abbr.3)
16. Risk treatment that involves deciding not to undertake a particular activity,(5)
17. Framework for identifying an organization's risk of exposure to internal and external threats which include disaster recovery, business recovery, crisis management, incident management, emergency management and contingency planning, (Abbr.3)
18. Results in decrease in net income on P&L statement,(4)
19. Colour generally used to rate levels of risk as low, (5)

PAGE INTENTIONALLY LEFT BLANK

PAGE INTENTIONALLY LEFT BLANK

PAGE INTENTIONALLY LEFT BLANK