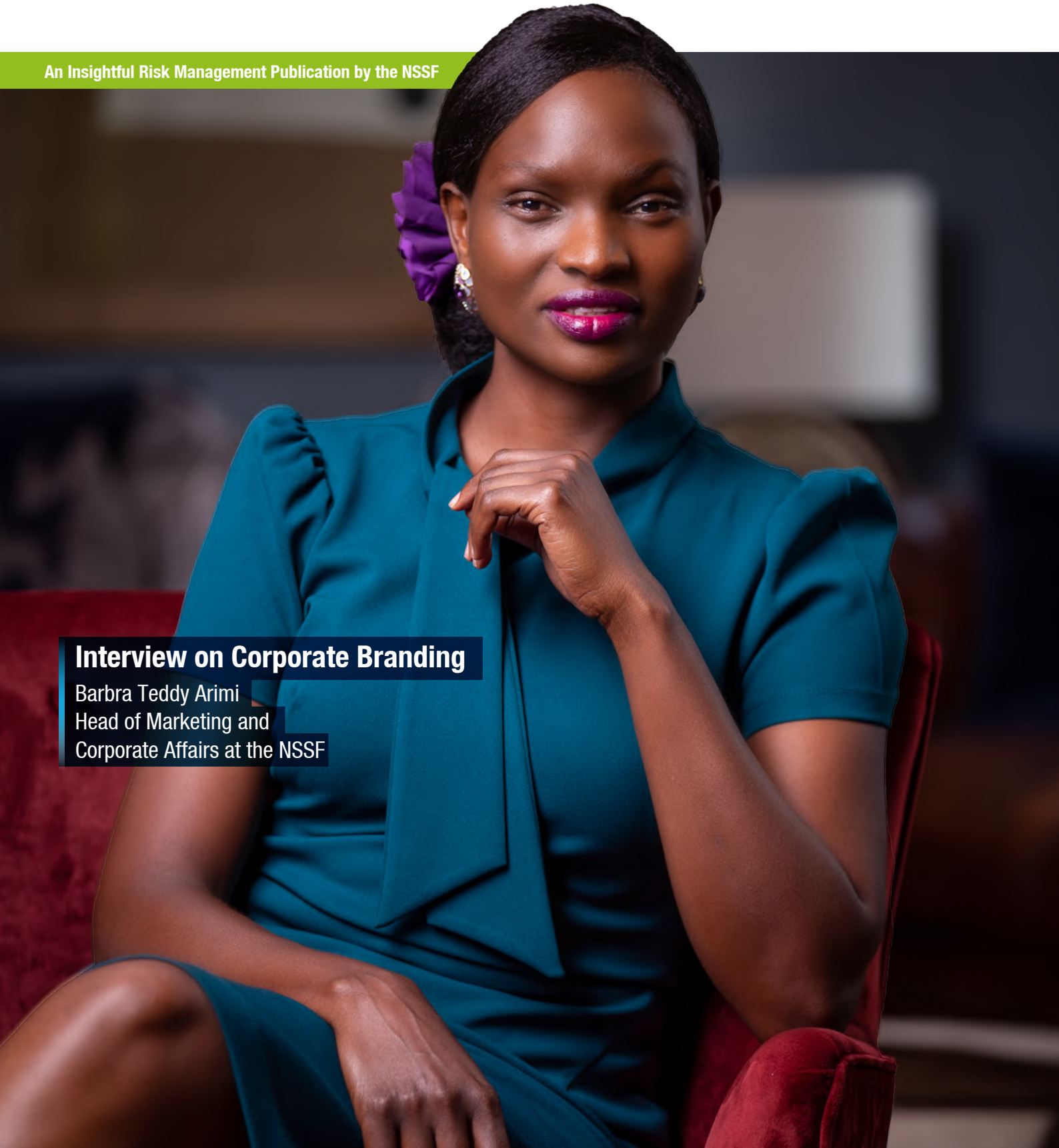
ISSUE FIVE I JUNE 2022

# The RiskEcho

An Insightful Risk Management Publication by the NSSF



## Interview on Corporate Branding

Barbra Teddy Arimi
Head of Marketing and
Corporate Affairs at the NSSF

# Foreword

***EDWARD SENYONJO***
***Head of Enterprise Risk Management,***
*National Social Security Fund*
*MBA, FCCA, CPA, BCOM, CERM*

Since our last issue in January 2022, the major risk event that has impacted the entire world is the ongoing Russia–Ukraine war. As life was beginning to return to normal, following significant decline in the Covid–19 infections in most parts of the world, the world was to experience yet another global crisis, this time not a pandemic but a war– Russia against Ukraine.

Although to many, the reasons for Russia's attack on Ukraine may not be clear or justifiable, the effects of the war are clear and felt by everyone around the globe. The attack on Ukraine by Russia prompted America and it's European allies, to institute stringent trade and diplomatic sanctions against Russia.

Consequently, Russia is unable to supply the much needed commodities around the world such as oil, gas, fertilizers, wheat, etc. Note that Russia is the third largest global producer of oil, after the US and Saudi Arabia, accounting for 10% of global supply. This has created global shortages, particularly of oil and gas, and has led to high inflation in many parts of the world, including the USA–8.3%, UK–7%, Germany–7%, Turkey–70%, Brazil–12%, etc., as at 30th April 2022. These are the highest inflation figures in 40, 30, 41, 20 and 19 years for the USA, UK, Germany, Turkey and Brazil, respectively.

What this means for business is increased cost of operation; every business needs to find ways to manage the escalating costs of doing business, short of which, profitability and growth will be compromised.

It is important to note that crises are likely to emerge from time to time; what is crucial is to be able to manage the crisis and protect your corporate brand.
Speaking of corporate brand, I am delighted to introduce to you M/s Barbra Teddy Arimi, the Head of Marketing and Corporate Affairs at the National Social Security Fund (NSSF), speaking about corporate branding and what makes the NSSF brand tick, in an exclusive interview on page 4.

Barbra is a business executive, whose experience spans the financial services sector, fast–moving consumer goods and academia. Her areas of expertise include marketing strategy, communications strategy, product development, brand management, research, public relations, and corporate governance.

Besides the interview, you will find many other exciting articles for your reading pleasure. Thank you for taking time to read this issue of *The Risk Echo*.

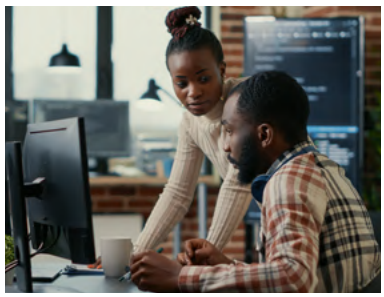
# CONTENTS











INTERVIEW ON CORPORATE BRANDING WITH

# Barbra Tedd

## Head of Marketing and Corporat

> Building a reputable
> one–day job, it take
> and effort, however,
> be done ove

**Firstly, our readers would like to know who Barbra is. Could you introduce yourself?**

I am a business executive, whose experience spans the financial services sector, fast–moving consumer goods and academia. My areas of expertise include marketing strategy, communi–cations strategy, product development, brand management, research, public relations, and corporate governance.

Currently, I am the Head of Marketing and Communications for the National Social Security Fund (NSSF), I also serve as a board member of the dfcu group and CEO apprenticeship board.

I am passionate about creating value; this entails adding value to the people I work with, which is then translated into value for customers and ultimately for the organizations that I have had an opportunity to serve.

**As a Head of Marketing and Corporate Affairs, talk to us about your key role at the NSSF**

Everything I do fits into our department's mandate, which is to build the Fund's brand and support the delivery of the business growth objectives of the Fund. This entails developing and supporting implementation of product devel–opment and research, public relations, corporate social responsibility and digital, and marketing and brand strategies, in collaboration with my colleagues in the department.

**What is branding and how is it important to a business?**

Many businesses aspire to stand out from the crowd. They have a desire to look and communi–cate distinctively from whoever else is doing the same or a different business. So, branding can be defined as an act of establishing an identity or image for an organization.

Branding is one of the drivers of the contempo–rary blue ocean strategy. It provides a robust branding strategy that positions a business to offering unique market propositions that usually derive competition within itself instead of competing against external players.

One of the most obvious reasons why businesses need branding, is to help them get recognized more often and gain trust from their customers. If you have a strong brand for your business, the market will naturally take note of it much more than they would a business without it.

A business that doesn't really have any cohesive brand identity for its products and services isn't going to stay in someone's mind for long. Like Tom Goodwin says, "Brands are essentially patterns of familiarity, meaning, fondness, and reassurance that exist in the minds of people."

**What does it take to build a strong brand?**

Consistency is key in building a strong brand. Once you have established your identity, and culture, then you must ensure your communica–tion is consistent to create top of mind awareness of your target group

You also need to get buy–in from the board and

# Q & A

# ly Arimi

## e Affairs at the NSSF

e brand isn't a
es a lot of time
destroying it can
ernight.

management, as these can act as your internal brand ambassadors, and in so doing, you influence the internal brand building aspect.

**The culture of an organization affects almost everything in the organization. In what specific ways does culture affect corporate brand?**

Organizational culture is usually reflected in the way employees treat or engage with customers. If the culture is lax, then you will find the same attitude exhibited when handling customer issues, and that's what that brand will be known for in the long run. So, an organization should deliberately create and drive the desired culture to align its employees with its brand values.

**What are the salient features of a brand that one needs to be aware of and harness?**

Every brand needs to be aware of the following.

**Brand promise:** This is the experience that a customer expects to receive every time they interact with your organization.

**Brand definition:** This describes what your business is i.e. who you are, your product offering/ solution and your customer.

**Brand positioning:** This is the uniqueness that sets your brand apart from the rest. You must carefully craft a strategy of how you want the customer to remember your brand.

**Brand personality:** This is like the human component of your brand. Meaning the traits that you want your brand to be known for, inside and outside the organization.

**Brand identity:** This is the visual aspect of your brand or what you'd call the *"look and feel"* However, consistency in all these aspects is what will make your brand strong.

**Membership to the NSSF is generally a legal requirement. Why is it necessary to undertake marketing at the NSSF?**

Any entity that provides a good or service to a customer, must undertake marketing to create value for the business; this value is in form of brand and business growth.

**Several years ago, the image of the Fund was badly tainted by corporate governance scandals. But like Walter Landor said, "Prod–ucts are made in a factory, brands are made in the minds". How have you been able to positively change public perception about the NSSF?**

A brand promise must be underpinned by delivery if you are to improve on your brand perception.

At the NSSF, we have underpinned our brand promise of a "better life" to our members through better delivery to our members across all fronts. We have delivered better returns to our members, improved our accountability and transparency, ensured a multi–channel approach to service delivery, improved product and service offerings, made better investment decisions and improved communication. In doing this consistently, we have built trust in our membership.

Our efforts have paid off; currently, the Fund's reputation index has grown to 73% as per the last internal brand health findings, and brand health has significantly improved from 66% to 80%.

**What are the critical success factors for a company seeking to rebrand itself?**

Corporations of whatever size grow and mature, and if this growth is not managed well, they tend to lose their spark, become complacent and easily die away. In the recent past, we have seen global corporations like Facebook rebrand to Meta, CBA to NCBA in the East African region, and The New Vision to New Vision Uganda.

In most instances, rebranding seeks to birth a new identity for the institution in terms of corporate vision, mission and goals; including the corporate and brand strategy, among other aspects. The entire process ushers in a new way of doing things in the organization. The reasons mostly revolve around provid–ing a stronger competitive edge in the marketplace to steer growth and brand appeal.

It is always advisable that all stake–holders, especially staff and the entire value chain are fully involved before, during and after the rebranding process.

The rebranding process can sound to be a simple process, but it is a painstaking process of changing the brand's corpo–rate identity altogether. If I may use a case study of Facebook rebranding to Meta last year in October, we learn five critical success factors from their rebranding:

**i) Leadership**

Leadership commitment plays a critical role in a rebranding process. The leadership of the entity needs to be clear about the reasons for undertaking the exercise; it reflects in the process and seals its fate. Hence, the top brass must take it upon its shoulders to give the campaign a direction. However, top executives can ensure positive brand reforms only if they listen to all the stakeholders involved in the exercise.

Elements like accommodating new ideas, taking an innovative approach, and forming a corporate strategy that's not limited to traditional methods, make for strong leadership that can take the right course of action.

**ii) Planning**

We also learn that building a comprehensive solid plan is a critical success factor; it should include everything such as a brand strategy, and consists of everything from the launch to pre–event and post–event activities — basically, it is a strict calendar with checkpoint deadlines for each division, department, section, etc. to reach its final goal.

**iii) Communication**

There must be a strong communication strategy conveying the new positioning of the organization to the target audience. It will only be effective if you have identified empirical data on customer insights, good enough to influence your target market in the new era.

**iv) Marketing strategy**

The other key success factor is the adoption of the right marketing strategy for all stakeholders across the board, as this is the cornerstone of the rebranding exercise.

**v) Lessons from other rebranding stories**

Lastly, there is a silent rule of thumb that points to corporations seeking to rebrand to study previous rebranding stories for the purpose of learning from their experiences to avoid the shortfalls.

**Currently, what are the key challenges facing the NSSF brand and how are you tackling them?**

Other than the historical governance issues, which have been practically addressed but still linger in the minds of some people, the key challenges are now majorly around regulations, which are beyond our control.

For example, the issues surrounding the statutory instrument on midterm access. Our strategy here is continuous sensitization of our members, both existing and potential, on the new regulations and the NSSF Amendments Act, as well as articula–tion of the new opportunities provided by the amendment Act.

**Briefly explain the key elements of your brand strategy that have put the NSSF among the top brands in the country**.

The NSSF brand is among the top– ranked brands in Uganda, it went through a rebranding exercise in 2011 that ushered in a renewed promise to its stakeholders. Since then, the NSSF brand has registered commendable milestones and achieved great success stories to date, among which is the brand appeal that signifi–cantly improved, which has been a key driver of the NSSF's growth.

We adopted a robust brand strategy that directly resonates with our customers; and some of the key elements therein include a broad under–standing of the business environment in which we operate, an organizational self–analysis framework, customer analysis and profiling to understand the needs and wants of our custom–ers, possible competing offerings on the market, the brand architype and persona, our brand essence and purpose, and lastly definition of our brand identity.

Our brand strategy is emphatic on appealing and connecting with our members in a way that creates a sustainable bond. This was a deliberate approach to lay the ground for a new brand promise to be accountable and transparent. This has made the NSSF brand trusted and has led to commendable brand performances over the years.

> "A deliberate approach to lay the ground for a new brand promise to be accountable and transparent. This has made the NSSF brand trusted and has led to commendable brand performances over the years."

Recent internal data has shown that more Ugandans would be willing to save with the NSSF even if the mandatory clause wasn't in existence, and are willing to recommend the brand to other people. This demonstrates the loyalty the brand has achieved over the years.

Our brand tonality and brand index for the first time reached 80% and 77% respectively, in the last 5 years compared to the past periods, when it was below 70%. Our corporate reputation Index now stands at 73%, which means we are a responsive brand to the society where we operate.

This is a testimony to the resilience of our brand strategy that has built a strong legacy in the market and in the country at large.

**How do you envisage the NSSF brand 5–10 years from now?**

The NSSF will be a household brand, synony–mous with social security, loved by most Ugandans in the formal and informal sectors. At this point, brand health will probably be higher than 80%.

**As a person in charge of product develop–ment, how are you positioning the Fund to take advantage of the opportunities brought about by the amendments of the NSSF Act to offer more products to its members?**

The opportunities presented by the NSSF Amendment Act include.

**Voluntary top–ups**

Members can increase their contributions beyond the 5%, this can help them increase on their accumulated savings, hence, enabling them to meet their savings goals.

**New benefits**

The Fund is developing additional benefits, in line with the Geneva Convention 102 on Social Security (Minimum Standards).

**Working population**

Every working Ugandan in the private sector can now save for their retirement with NSSF, since the initial threshold of five employees for eligibil–ity has now been scrapped.

We plan to run several campaigns in the near future that will clearly articulate these opportuni–ties.

**Your last comment on branding?**

Building a reputable brand isn't a one–day job, it takes a lot of time and effort, however, destroying it can be done overnight. We should, therefore, jealously guard our personal brands as well as the brands of the various organizations that we work for.

# ALIGNMENT OF INFORMATION SECURITY WITH ERM STRATEGIES

## An effective approach to cyber risk management



***STEPHEN BABIGUMIRA***
***Information Security Manager,***
*CISSP, CRISC, CISA, CEH, ISO 27001 LA,*
*ISO 27001 Lead implementor OCA, Msc.IS, BIT*

Information security risk, just like other risks, such as financial risk, operational risk, compliance risk, reputational risk, etc., affects the bottom line of an organization. It can increase operational costs and affect revenue and customer satisfaction. Due to its peculiar and dynamic nature, information security risk needs to be viewed as a strategic risk and aligned with the Enterprise Risk Management (ERM) strategies.

According to a recent survey by the Global Cybersecurity Outlook 2022, 92% of business executives surveyed agree that cyber resilience was integrated into enterprise risk–management strategies. However, a lower percentage (84%) of respondents shared the view that cyber resilience was considered a business priority in their organizations, with support and direction from leadership, but a significantly smaller proportion (68%) saw cyber resilience as a major part of their overall risk management.

Regardless of your perception about how cyber–security should be positioned within the risk space, the reality is that cyber security risk is becoming the biggest threat to businesses. Cyber–attacks and the consequential data breaches were not common in the past. Today, the tables have turned, cyber–attacks have grown in sophistication and frequency. For example, according to the World Economic Forum's Global Cybersecurity Outlook 2022, malware and ransomware increased by 358% and 435% respectively in 2020. The survey also indicates that as many as 80% of cyber leaders stressed that ransomware is a dangerous and evolving threat to public safety.

> **According to the 2022 Global Digital Trust Insights Survey by PwC, 69% of the respondents predict a rise in cyber spending in 2022 compared to 55% last year**

The cyber–attacks have driven a change in the way organizations view information security. Previously, it used to be reduced to a mere technology issue, but it is now recognized as a strategic business concern, which companies need to take as a priority. Information security has been taken out of the boundaries of IT to be an independent function that looks at security from a business perspective, encompassing processes, people and technology.

This trend is likely to continue as the importance of information to organizations continues to grow. Data is now regarded as the new oil. Companies are determined more than ever before to protect their data. This could explain the increased investments in information security by compa–nies as a measure to fend off threats towards the valuable information assets. According to the 2022 Global Digital Trust Insights Survey by PwC, 69% of the respondents predict a rise in cyber spending in 2022 compared to 55% last year.

By and large, the board and senior executives of organizations recognize the serious risks that cyberattacks pose to their business profits and reputation. However, they continue to struggle with creating strategies that help them under–stand and address the cyber risks. Cybersecurity is critical, but the panic it has created or contin–ues to create in board rooms has elevated it to the status of being the most misunderstood/ un–researched topic discussed in meetings.

Unfortunately, many inappropriate decisions on which tools, talent and processes to implement, are being made based on myths rather than facts or to comply to a certain standard or achieve a certain maturity level, without due consideration to business needs.

Often, when faced with a decision to invest in or implement a cybersecurity solution, management tends to approve it instinctively without a clear risk assessment and consideration of other alternatives. In such situations, the executives normally think that throwing money to the problem (cyber risk) will have it solved.

There is nothing like perfect information security or being safe from a cyber–attack, therefore attempting to implement every control that exists to stop every risk, will not only increase opera–tional costs but may also cause business disrup–tions.

For example, a large bank may be able to patch its systems within 3 days because the industry standards recommend so, but the downtime required may be unacceptable. Just implement–ing the industry standard requirements, which do not take into consideration the organization's specific constraints, that is, resources, internal policies, business needs etc., may have

far–reaching impact on the business.
Therefore, the best approach is to first identify the cyber security risk and then determine the appropriate security control, not just seeking to implement any control available on the market. Some risks are mitigated through compensating controls and not necessarily direct controls.

However, taking this approach would require that before a control is implemented, a proper risk assessment that takes into consideration all existing and compensating controls, is conduct–ed.

In addition, sometimes organizations tend to solve the wrong cyber security problems; ideally, solving a problem would require getting a clear understanding of it before any attempts to address it are undertaken. Implementation of controls should not be just a compliance issue but should be informed by offensive approaches. Finally, those entrusted with ensuring the safety of the organization's information assets often make a mistake of adopting a one size–fits–all approach towards managing cyber risk.

The notion of, "the cyber threats targeting similar organizations in my industry are also my threats", works well when conducting the threat hunting and threat intelligence in order to help organiza–tions create a comprehensive list of possible threats. However, different organizations will continue to have unique risks, different vulnera–bilities, different risk tolerances and risk appetite. So, the one–size–fits–all approach to managing cybersecurity risk is not appropriate.

The approach and practices must be customized, and the mitigation measures should be planned, designed and implemented in accordance with the organization's risk appetite, tolerance limits and enterprise risk management strategies to avoid nugatory expenditures.

In my opinion, the people entrusted to manage the organization's information security, should have a clear understanding of the organization's business risk drivers, risk appetite and risk tolerance limits, such that cyber risk approach is informed and guided by these three parameters.

A deliberate effort to incorporate information security strategy into the ERM strategy should be undertaken by management. This will help an organization to align and prioritize its information security activities with its business requirements and resources, such that it's the right risks that are addressed not myths, and that resources are optimized, not wasted.




***JESSE OKUTRE***
***Investment Risk Analyst ,***
*MBA, BECON, CERM, CRA,*
*ISO 270071 Lead Implementor*

# CLIMATE CHANGE: A SUBTLE VOLCANO THAT POSES A GREAT RISK TO HUMANITY AND BUSINESS

A lot has been written about climate change for a long time, but it is still one of those mysterious concepts that many don't appreciate. This is because the effects of climate change are usually gradual and long–term, oftentimes arising out of human activities on the environment. Since the effects are felt many years after the activities causing the change in climate, it is, therefore difficult for many to appreciate the linkage between human activities and climate change. The lack of appreciation of the linkage between the two exacerbates the problem and puts the planet at a heightened risk of climate change

When Donald Trump became the president of the United States of America, his administration withdrew from the Paris Agreement (An agree–ment where nearly 200 nations signed a deal with a promise to reduce greenhouse gas emissions), causing an uproar about the US's action of withdrawing from such a critical agree–ment intended to secure the future of the planet.

Fortunately, after Joe Biden was sworn in as the President of the US, the US was quick to rejoin the Paris Agreement and reunite with the 200 member states.

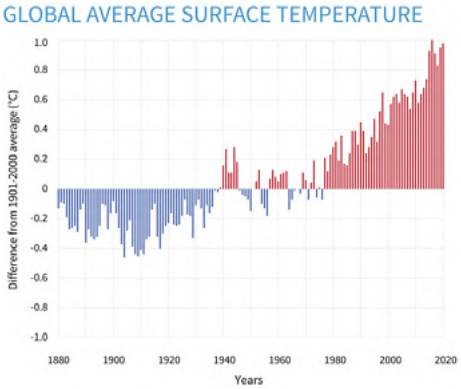
According to National Geographic, climate change is a complex shift affecting the planet's weather and climate system. The climate system includes solar radiation, temperature, humidity, precipitation (type, frequency, and amount), atmospheric pressure, and wind (speed and direction).

However, the effects of climate change manifest mainly through an increase in temperature (global warming), strong winds (cyclones, tornados, hurricanes, and typhoons), and heavy rainfall (causing flooding).

**Effects of climate change on the environment**

**a) Global warming**

The increase in the planet's temperature is a phenomenon called global warming.




*Source: www.climate.gov*

The average global temperature has increased by 2 degrees Fahrenheit, from 1900 to date(See the graph above). According to weather scientists, the increase in temperatures is not likely to stop anytime soon and will have adverse effects if nothing is done to reverse the situation.

Global warming is responsible for prolonged dry seasons in many parts of the world, leading to droughts, which cause death of millions of animals due to scarcity of water and pasture, and the destruction of plant species around the world.

Global warming also causes health issues such as respiratory infections, prevalent malaria cases, etc, and has adverse effects on agricul–ture, resulting in low crop yields and conse–quently widespread hunger (low agricultural produce due to prolonged droughts and extreme rainfalls).

**b) Flooding**

Floods happen in many forms:

(i) An overflow of coastal lines and riverbanks, and excessive water on the dry land that cannot be absorbed. Floods are expected to continue in the future and even become severe.

ii) Global warming, which is the increase in global temperature, causes the glaciers, snow, and icebergs to melt and make the atmosphere

damp, causing an overflow of rivers, oceanic coastal lines, and hefty rainfalls.

Floods are very destructive, causing death to humans and livestock, destroying infrastructure, and causing famine.

**c) Strong winds**

According to the Scientific American website, the average wind speeds have increased from 7mph to 7.4 mph in less than a decade. This is expect–ed to increase with the increase in global temperatures. Weather scientists anticipate that, with the rise in pollution and adverse human activities, the wind speeds will increase. The brisk winds can be destructive and can raze cities to the ground.

*Strong winds blowing tress in Chip Somodevilla (Getty image).*

In Uganda, we have seen the effects of global warming in various forms;

(i) We have experienced extreme rainfalls that have affected agricultural production and

(ii) Long and scorching dry seasons, which have affected farmers' income, thus their livelihood.

(iii) The landslides in the Rwenzori region and Eastern part of the country have significantly destroyed infrastructure and caused deaths in some cases.

*Landslides in Bududa, Eastern Uganda (www.trtworld.com/)*

We have also seen floods in Kasese when it rains. These are no doubt the effects of global warming

**Impact of climate change on business**

Global warming translates into financial risk for businesses, and it can manifest in several ways, including:

**i) Market conditions (supply and demand) risk**

Extreme climate events are known to influence supply and demand. According to the Interna–tional Finance Corporation (IFC), rising tempera–tures due to climate change will decrease winter heating demand and increase summer cooling demand. In Russia, it is estimated that a 2°C temperature increase will decrease fossil fuel demand by 5–10 percent and electricity demand by 1–3 percent. Winter heating demand in Hungary and Romania is expected to fall in warmer winters by 6–8 percent by 2021–50 (IFC).

**ii) Decrease in productivity and reduction in output, leading to a loss in revenue**

Changes in rainfall patterns affect rivers, which affects hydroelectricity production. Power shortages affect the production and supply of products. For example, in the West Nile region of Uganda, there is an acute shortage of hydroelec–tricity during the dry season; power is rationed, and businesses rely on diesel–powered genera–tors for electricity. This increases the cost of doing business and leads to loss of revenue.

**iii) Transition risk**

This risk arises from a company's response to climate change, such as changes in technolo–gies, markets, and regulations that can increase business costs, undermine the viability of existing products or services, or affect asset value. In countries with a high level of climate–change consciousness, companies have embarked on the green movement, where the fight against climate change is considered, for instance, in issuing loans, attracting investors, etc. Compa–nies are being forced to change their mode of operation and policies to cut greenhouse emissions.

For example, financial institutions and rating agencies (S&P500), Moody, etc.) are being pushed to incorporate climate change into the credit risk rating models for risk management.

That means, borrowers will be asked about their plans for fighting climate change, which might affect their credit scores, and country credit risk ratings will also be affected by the country's policies to fight climate change.

**iv) Increased capital and operational expen–ditures**

Extreme rainfalls due to global warming can negatively affect the physical infrastructure. The heavy rains that last 6 to 8 hours lead to landslides destroying roads, houses, crops and livestock.

A year back, the landslides in Kasese, in Western Uganda, led to the destruction of roads (Kihara–Kapoko road) and other properties.

In countries where storms and hurricanes are common, companies are increasing insurance costs. According to the international Finance committee, Oil and gas companies that operate offshore have to increase insurance costs to cover plants at the shores. Such incidences increase the company's operational and capital expenditure.

Increases in temperatures accelerate the depre–ciation of assets. Due to climate change, the wear and tear of assets and infrastructures are considerably faster, leading to an overstatement of useful life and values of assets. This means that the capital expenditures will increase within a short time due to asset replacement.

**v) Staff health, safety, and productivity**

With the global temperatures anticipated to keep increasing, this may impact the health, safety, and productivity of employees. According to IFC,

higher temperatures can have consequences on workers' morale and productivity; and very extreme temperatures can result in potentially fatal heat stress.

According to S.D Fernando (Professor at the Department of Parasitology, Faculty of Medicine, University of Colombo, Sri Lanka), an increase in temperature, rainfall, and humidity may cause a proliferation of the malaria–carrying mosquitoes at higher altitudes, resulting in an increase in malaria transmission in areas in which it was not reported earlier.

**vi) Reputational risk as a result of ignoring climate change effects**

Climate change has been identified as a potential source of reputational risk related to changing customer or community perceptions of an organization's contribution to or detracting from the transition to a lower–carbon economy.

For example, according to the businessinsid–er.com, the Hummer SUV and truck, a civilian model of the Humvee (US Military), used to be a popular vehicle driven by celebrities and wealthy individuals. However, the glory of the Hummer was short–lived, as climate activists identified it as a gas guzzler, which was claimed to acceler–ate global warming.

Riots broke out throughout the US, affecting the reputation of the Hummer; a reduction in sales followed since whoever owned it was either attacked by rioters or vehicle destroyed.

**Mitigating Climate Change**

Information about how climate change can be prevented is available in the public domain, here I will re–echo the United Nations Environment Programme's ten ways through which you help fight the climate crisis.

**i) Spread the word**

Preach the word about climate change to family and friends, encourage them to join the fight to prevent global warming. Join globally organized climate change movements and challenges such as "Count–Us–In" and the "#Act–Now" campaign.

**ii) Keep up the political pressure**

Lobby local politicians and businesses to support efforts to cut emissions and reduce carbon pollution. Using leaders would help combat climate change, they are the decision–makers

and influencers in the community.

**iii) Transform your transport**

Transportation contributes to a quarter of the greenhouse emissions. Decarbonizing the cities by encouraging transportation modes that eliminate carbon emissions, such as using bicycles and walking, is good for the fight against climate change.

**iv) Rein on power use**

Families and companies should be encouraged to consider using zero–carbon or renewable energy providers, e.g. using solar panels, switching off appliances and lights, and using the most efficient energy products (eco–friendly bulbs, fridges, ACs, etc.)

**v) Tweak the diet**

The population should lean towards eating more plant–based meals than animal–based meals, which are unhealthy and most common around the globe.

**vi) Shop local and buy sustainable**

Support local businesses and farms; this reduces fossil fuel emissions that are associated with transportation and the supply chain. Sustainable agriculture uses up to 56% less energy and creates 65% less emissions. All these are aimed at reducing the carbon footprint.

**vii) Don't waste food**

According to the Food Waste index report 2021, 1 billion tons of food is wasted, contributing to 8–10 percent of greenhouse emissions. Buy food that is enough, make use of every eatable part of the food you purchase, and store food correctly.

**viii) Dress (Climate) smart**

The fashion industry accounts for 8–10% percent of global emissions, and with "fast fashion" trend, a throwaway culture has been created, in which clothes are quickly deposed off.

This can be mitigated by using a few clothes for a more extended period (which saves money) and renting clothes for one–off functions and parties (weddings, graduations, etc.).

**ix) Plant trees**

Deforestation is happening on a massive scale due to the need to have land for agriculture, timber (furniture and construction), and human settlement. UNEP estimates that 12 million hectares of forests are destroyed every year.

Taking a personal initiative to plant trees and maintaining a green environment is the only way this fight can be won.

**x) Investing in planet–friendly investments**

This is a deliberate move by individuals to invest or make purchases that save the environment, e.g. buying re–cyclable products, using petrol cars other than diesel, investing in renewable energy, eco–friendly vehicles (hybrids), and companies with eco–friendly policies, etc.

**Conclusion**

It is important to note that the effects of climate change are usually long–term but oftentimes catastrophic, and no human force can stop them when they begin to manifest. The good news is that many preventive measures, such as those explained above, are not too complicated for anyone to adopt. The choice is now up to every–one, whether to choose self–destruction or self–preservation.


# CONTROL SELF–ASSESSMENT (CSA): A CRITICAL TOOL FOR CONTROL ASSURANCE

***ADOLF BAGUMA KAIJA***
***Operational Risk Manager,***
*MBA, CPA, BCOM, CERM*

Control assurance is a critical element of an effective risk management framework that helps provide organizations with objec–tive evidence that controls have been designed, and are operating effectively within the risk tolerances set by the board.

Control assurance supports the organi–zation to ensure that strategic, tactical and operational risks are effectively managed across the entire organiza–tional value chain.

Typically, control assurance activities have, over the years, been a preserve of the audit function across many organi–zations. It has, however, been long argued that auditing cannot provide absolute assurance because an audit is usually done on a sample basis– the auditor does not check everything, among other reasons. Therefore, the audit, even if conducted in accordance with generally accepted auditing standards, may not detect certain misstatements.

Dissatisfied with the level of effective–ness of audits conducted at the end of specified business cycles, in 1987, Gulf Canada developed a new technique of evaluating controls by the process–owners, which they called Control self–assessment (CSA).

The control self–assessment technique is a business practice that helps organtions identify and appraise significant risks inherent within the organization's processes or activities on a day–to–day basis, in contrast to the traditional audit, which is done periodically.

A number of organizations, including the National Social Security Fund, have since adopted and implemented this model as part of an integrated control assurance framework, where, maximum assurance could be attained by involving every body across the organization.

In contrast to the traditional auditing techniques, the CSA framework seeks to encourage staff, whose day–to–day responsibilities are within the business unit being considered, to evaluate the adequacy and effectiveness of controls associat–ed with the risks within their areas of operation.


**Benefits of Control Self–Assessment**

Although the real or perceived benefits of the CSA technique may vary among organizations, it goes without saying that organizations could enjoy several benefits from the model, if well implement–ed, such as the ones explained below:

**a)** Control self–assessment creates a clear line of accountability for controls, reduces the risk of fraud by examining data that may flag unusual patterns of transactions, and results in an organization with a lower risk profile.

**b)** The CSA model works as a precursor for internal and external audits, which are generally conducted at the end of the activity implementation.

**c)** Staff participation in the assessment of their internal controls helps develop a sense of ownership of the controls. This, in most instances reduces resistance to control, improvement, initiatives among the process or activity implementers

**d)** Provides reasonable assurance to Management and other stakeholders that internal control systems of the organization are effective.

**e)** Helps in evaluating the likelihood of achieving the business objectives and increases awareness of risk and internal controls among staff.

**f)** The control self–assessment model creates a better understanding of business operations, reinforces stronger awareness of risk practices and improves control effectiveness.

**Effectiveness of Control Self–Assessment**

Like any other business process, control self–assessment cannot be without its own downside including but not limited to;

**i.** The assessment is conducted by the very individuals who are responsible for implementing the controls; and it would be argued that they are likely to be biased and fail to make objective assessment of the controls.

**ii.** Staff who perform the CSA procedure may also not have adequate competencies in providing assurance on the relevant processes.

**iii.** The individuals performing the assessment to verify that key controls are functioning properly, may not recommend improvement because any adjustments in the process could slow down the speed at which activities are executed, and hence increase the turnaround time.

While the above shortcomings may exist, organizations can devise ways on how to improve the downside of the control–self assessment model and make it more effective.

One of the most effective ways of improving the CSA process is to improve on the corporate risk awareness and culture, where individuals managing and evaluating their own controls understand the importance of providing an honest assessment.

Let me now share with you what the National Social Security Fund risk management framework has devised to improve effectiveness of the CSA model.

**1) Creating awareness**

The CSA process begins with creating awareness through regular face–to–face training/–sensitization, and use of risk bulletins and other forms of disseminating of risk management information. Risk awareness raises an understanding of which risks exist, their potential impacts, and how they should be mitigated. Organizations must ensure that employees are aware of current and potential risks in the workplace, as well as the relevant controls in place to mitigate those risks.

> **For an organization to have an effective risk management framework, the first step is to identify the various risks the organization is currently facing or could face in the future.....**

**2) Determining organizational risk profile/risk registers**

For an organization to have an effective risk management framework, the first step is to identify the various risks the organization is currently facing or could face in the future. This process is conducted by holding workshops with the different business units/process owners throughout the organization, to brainstorm and come up with the risk universe and the relevant control actions, which culminates into risk registers.

Risk profiling begins with identifying all the business processes and a critical examination of all the different activities under each process to enable the team figure out all possible impediments to the achievement of the objectives under each business process.

**3) Structure of the CSA**

The criterion for assessing controls is based on two parameters:

i. Control design
ii. Application of the control

**i) Control design.**

The control design is a pivotal part of the risk treatment stage in the risk management process. The design of a control is basically about how the control is intended to function, and the extent to which it mitigates the risk. Those conducting the assessment seek to find out whether the control is adequate, partially adequate or inadequate. If the control is partially adequate or inadequate, an additional or alternative control(s) is/are provided.

**ii) Application of the control**

After assessment of the control adequacy, an assessment of the application of the control is carried out, seeking to establish whether the control is consistently applied, seldom applied or not applied at all.

The significance of evaluating the application of the control is that, if a control is not consistently applied as intended, regardless of its adequacy, it won't be effective in mitigating the risk. An effective control is one which is adequate and is consistently applied.

Let's take an example of a padlock, which is meant to prevent unauthorized access into the building. Even if the padlock is one of the best quality on the market, the unauthorized–access vulnerability will remain, for as long as the door is not locked consistently.

**4) CSA programme**

**4.1 Communication and execution of the program**

A programme for the CSA exercise is then drawn and communicated to all stakeholders to help them plan for the execution of the CSA exercise.

**4.2 Validation of CSA & remedial actions**

Once the CSA has been completed, an indepen–dent team from the Risk function follows through with the control owners/assessors to validate the integrity of the CSA responses. Conducting control self–assessment validation helps to improve the integrity of the CSA exercise.

The validation exercise entails sitting down with the process owners to evaluate the evidences available to confirm that their control self–as–sessment results represent the actual results on the ground. This helps to test the validity and reliability of the CSA results and improves the integrity of the exercise.

**"An independent team from the Risk function follows through with the control owners/assessors to validate the integrity of the CSA responses. Conducting control self–assessment validation helps to improve the integrity of the CSA exercise."**

**5) Control rating**

After the validation exercise, every department's performance is evaluated based on how many controls have been assessed as effective in relation to the total number of controls in its register.

The average score for all the departments is taken as the organization's score. The depart–mental and organizational scores are incorpo–rated in each staff's and the Managing Director's balanced scorecards respectively, as KPIs (Key Performance Indicators).

**6) Communication of CSA results**

The results of the exercise are then discussed and communicated to all business units.

**7) Tracking of remedial action**

All the controls that are rated as ineffective in terms of their design and/or consistency of application are communicated to risk owners and remedial actions agreed. The Risk team then monitors the implementation of the agreed actions.

**Conclusion**

The process of continual evaluation of risks and controls, and making plans to mitigate and/or eliminate the risk is a powerful tool in strength–ening internal controls, complementing the traditional assurance frameworks as well as improving the overall control environment in the organization.

The control self–assessment approach provides a broad perspective of controls, where all stake–holders participate and contribute to the control assurance process, creating a culture of contin–ual improvement.

# INTRODUCING THE NEW
# NSSF SMART CARD

It's your NSSF account, your *bank and loyalty benefits, **all 3 in 1 card.**
Upgrade to the **new NSSF Smart card** and experience a new level of possibilities.

Apply for yours now, visit the **NSSF branch** at **Workers House** or any **Centenary Bank Branch.**


For more information call **0800 286773**
or **visit www.nssfug.org/smartcard**

**#DoMore** *Terms and conditions apply.

Powered by Centenary Bank ...our bank

NSSF SmartCard™

# THE NEED FOR COMPANIES TO RESHAPE THEIR ERM STRATEGIES

***ROBERT MASIGA***
***Operational Risk Officer,***
*BSTAT, CFA Level 3*

From the Covid–19 pandemic to the Russia–Ukraine war, with the most comprehensive sanctions against Russia, which have disrupted global supply chains and caused global inflation, with a likelihood of culminat–ing into a third world war, the world is experiencing a period of unprecedented turbulence.

That aside, globalization, new technol–ogies, geopolitical dynamics, changing customer needs, cybercrime, and climate change, are some of the factors that have combined to overturn the business environment and give many business leaders a profound reason for discomfort. Under these circumstances, many companies' risk management strategies have been undermined and may need to be reshaped.

Operating terrains have greatly shifted. Formerly, organizations that had been in business for many years with a strong market share, were viewed as 'giants' regardless of their risk management models.

The order of the day, then was, once a control was designed, the attendant risk was considered mitigated for years. They did this for decades without paying attention to other external environment, and companies like Kodak are now defunct.

The contributing factors to the changing operating environment that necessitate change in the Enterprise Risk Manage–ment (ERM) are many, but here I will highlight just some of them.

**Globalization**

This phenomenon has introduced many aspects in the business environment, most importantly, opening businesses to new markets, changing in multiple dimensions the way nations, businesses and people interact, by removing barriers set by both geographical and political boundaries.

This presents opportunities as well as risks. Take an example of a company which is a monopoly in the market; once the economy opens to external players, the company faces competition. For products that are highly–priced, it becomes inevitable to lower their prices in order to maintain customer base, or else customers will find alternative products from the competitors.

Also consider a situation where the sources of raw materials used are purchased expensively, just because of lack of alternatives. Should the market open up, cheaper sources will be identi–fied.

The above scenarios provide the need for chang–es in the business processes; and usually the new changes will present new risks, which will require new controls. Companies that assume that old controls will be effective in the new environment, will soon be part of history.

**Cutthroat competition**

The ever–increasing competition brought about by opening up economies globally, is enabling companies to enter offshore markets. Respond–ing to increased competition, companies are forced to look for opportunities in foreign countries to optimize profits.

This, however, increases the companies' risk profiles, ranging from political, economic, social, and technological risks. The manifestations of these risks come in different forms, such as differences in regulations, culture, language, locations, time zones, currencies, among others.

Moving into foreign countries may render some controls in the parent country not applicable across the new establishments. This will, therefore, require designing new controls appro–priate for operations in different countries.

**Emerging technologies**

The emergency of e–business created huge opportunities for market access globally, and businesses are becoming increasingly intercon–nected to suppliers in global markets.

Formerly, a message took days to be delivered across; currently it can be delivered in a blink of an eye! The most remarkable technological change in business, in my view, is in the field of payment. Before the advent of the new payment systems, money to reach its intended recipient necessitated physical movement. Nowadays, everything can perfectly be done online, anywhere at one's convenience, using methods like EFT, RTGS, mobile money, etc.
Relatedly, one can ably work for an overseas company while based in another country, which can be thousands of miles away; all made possible with advancements in technology.

However, changes in technology have increased risk exposure for organizations in a number of ways. One such important risk to note is cyber security risk. Organizations have inevitably become dependent on computers and internet services regardless of their sizes. This is contrary to how the mode of operation was in the olden days. For instance, in the nineteenth century, it was rare for a company to own a computer. Today, even a kindergarten child can own and operate a comput–er. This, therefore, has increased the risk surface in terms of cyber–attacks.

This calls for a redesign of organizations' ERM practices like hardening the potential targets and fixing the vulnerabilities to limit the attack surface, having senior management team getting involved in cyber security risk management and incorporating ERM in the organizations' overall business strate–gies. This will go a long way in helping organiza–tions to improve their ability to detect and respond to events that threaten their physical and technolo–gy systems.

> **"In the nineteenth century, it was rare for a company to own a com–puter. Today, even a kindergarten child can own and operate a com–puter. This, therefore, has increased the risk surface in terms of cyber–attacks.**

**Geopolitical Dynamics**

Geopolitical tensions have resulted in serious ramifications on business operations. Many companies around the world have often failed due to geopolitical contentions between their host countries and their counterparties (coun–tries), with their counterparts, which has result–ed in unfavorable trade terms, wars etc. This has not only affected small economies but also big ones.

America and China have had disagreements over time, which escalated during the Trump admin–istration. Currently, a host of companies have either withdrawn or suspended their operations in or with Russia due to the Russia–Ukraine crisis, for fear of secondary sanctions from the US and/or its European allies. In East Africa, Uganda has had trading issues with her neigh–bors such as Kenya and Rwanda. All these combine to cause changes in the operating business environment, which might include a shift in strategic partnerships.

The next era of geopolitical change is increas–ingly becoming uncertain, which should force business enterprises to make deeper assess–ments and adjustments to geopolitical risk rating, which are essential in resource allocation for business continuity.

The current pace of political events around the world requires that corporate executives take the initiative to confront the consequences of the links between geopolitics and business perfor–mance.

**Changing customer expectations**

The ability to meet the ever–changing customer expectations and need to consistently exceed those expectations is a critical concern for many organizations. To this end, customer expecta–tions have substantially changed. Turnaround time for customer's product/service delivery is one major concern that clients have become more critical about. Further, the world having become a global village, people continually experience changes in knowledge and priorities. It should be remembered that for any business, sustainability, customer retention, growth, and relevance, are critical requirements for its continued operations. Hence, these need to be an integral part of the overall business opera–tions and strategy.

Constant evolution of customer demands and the need for organizations to position their businesses, calls for an adaptation of their marketing and production mix to continue to be effective at meeting their customers' needs.

Efforts to address these evolving customer

demands, invite a new set of risks, which altogether require a new set of controls; and this calls for continuous innovation and agility.

**Climate change**

The effects of global warming, caused by human activities are felt across the globe in form of prolonged droughts and high temperatures, flooding, strong winds, accelerated sea–level rise, changes in the rain patterns, etc. All these combine to cause havoc and hence, a lot of sufferings to people and their property.
These changes are projected to worsen in the decades to come. For that matter, therefore, businesses need to get prepared to address hazards that have occurred and are bound to continue occurring in the future.

These climatic changes, have multiplier effects on the crystallization of several risks, including but not limited to famine, malnutrition, human displacement, increased insurance premiums, increased new infrastructure requirements, etc., all of which can substantially affect the opera–tional landscape.

The climate volatility is forcing companies to redraw their corporate risk management strate–gy. Companies are facing numerous risks, ranging from physical risks in terms of property destruction, to policy and/or regulation changes. This, therefore, undermines the traditional risk management strategies, which should be redefined or augmented to address the new challenges that emerge every now and then.

In conclusion, therefore, time is up for any company, regardless of its size, to have its risk antennae signal tuned to changes in its operat–ing environment in order to survive the turbu–lence. This requires companies to act quickly to enhance or reinvent their business models and even reshape their enterprise risk management landscape.

# RISK APPETITE– AN INVISIBLE HAND IN DECISION–MAKING

The word appetite is ordinarily used to mean the desire to satisfy a human need, and is more commonly used for the desire for food. Risk appetite is not so different, only that it relates to risk.

The Committee of Sponsoring Organizations of the Treadway Commission(COSO) defines risk appetite as the amount of risk, on a broad level, an organization is willing to accept in pursuit of value. If this is written down, then it forms what is called a risk appetite statement.

The willingness to accept certain risks means that a risk appetite is a matter of choice, and different people make different choices. The choice is important because risk capacity is not limitless, and different people have different risk–return preferences.

Risk appetite is particularly important for effective corporate governance, as it prescribes spheres of operation for manage–ment. The board does not participate in the day–to–day operations of the organization; by setting clear "boundaries" (risk appetite), the board is able to influence the decisions of management, which must be made within the risk appetite of the organization. The key question to ask, therefore is, is this matter under consideration within our risk appetite?

***EDWARD SENYONJO***
***Head of Enterprise Risk Management,***
*MBA, FCCA, CPA, BCOM, CERM*

It is worth noting that the purpose of a risk appetite statement is not to stop the organization from taking risks, as taking risk is the source of creation of value. As Denis Waitley said, "Life is inherently risky. There is only one big risk you should avoid at all costs, and that is the risk of doing nothing".

As mentioned earlier, different organizations have different appetites for risk. On the continu–um, there are two extremes; those that have high appetite for risk (Risk–aggressive), and on the other hand those that have low appetite for risk (risk averse), and the majority fall in between. At a macro level, the private sector is generally risk–aggressive, while the public sector is risk–averse. The public sector deals with public goods, whose return or lack of it may not have a direct correlation with the cost of the investment. The private sector is driven by the forces of demand and supply; where the risk is high, the consumers compensate the producer highly.
However, it is important to note that both extremes can be dangerous, as excessive control cripples the business, while on the other hand, reckless risk–taking ruins the business.
Therefore, the biggest challenge that faces any business is how to strike an appropriate balance between risk and return/reward. The appropriate balance is the basis for an appropriate risk appetite statement.

The factors contributing to the variation in risk appetite by different organizations are varied, and include:

**Culture of the organization**

The culture of the organization, which is greatly influenced by the behavior and attitude of top management and the board, shapes the risk appetite of the organization. Like Ida B. Wells, a prominent journalist, activist, and researcher said, "appetite grows for what it feeds on". The behavior of individuals is influenced by their background (cultural, educational, professional, etc.), as in the words of Zig Ziglar, an American author, salesman, and motivational speaker, "What you feed your mind determines your appetite".

An organization's risk appetite is normally a broad level statement that encompasses the high–level risk profile of the entity. It is therefore, generally set through a top–down approach. Consequently, management which exhibits a "must–win–at–all–cost" attitude is likely to set a high risk appetite. For instance, tech compa–nies are generally known to be risk–aggressive, and this explains the dynamic nature of the tech industry.

Conversely, a risk–averse organization will be conservative in setting the risk appetite. For example, pharmaceutical companies are highly risk–averse. This is due to the fact that they deal with human life, and are highly regulated.

> **“ In order to stay afloat or be in the lead, many entities may be compelled to take aggressive approach to risk. That means the organization may adopt a high appetite for risk in an attempt to outpace its competitors. ”**

**Regulatory environment**

Regulators usually set boundaries within which business should be carried out. For instance, in the banking sector various credit, trading, and other limits are set to regulate the business of the financial institutions. In addition, the regulator defines the nature of business (and therefore the nature of risks), that the regulated financial institutions can undertake.

These limits act as barriers for risk–taking, as the financial institutions cannot, however risk–aggressive they may be, operate outside the limits set by the regulator. It is therefore, common to find financial institutions setting their credit limits below the regulatory limits, to avoid penalties/sanctions for non–compliance. This obviously limits their appetite for risk in that regard.

**Level of competition**

In a highly competitive environment, it is survival of the fittest; the slow ones lose the race. In order to stay afloat or be in the lead, many entities may be compelled to take aggressive approach to risk. That means the organization may adopt a high appetite for risk in an attempt to outpace its competitors.

**Recession/Crisis period**

During a period of low economic activities or during a crisis period, such as the Covid–19 period, organizations may take a cautious approach to risk. This is because the level of uncertainty escalates during such a period, and therefore, swimming in unchartered waters may escalate losses.

**How to develop an appropriate risk appetite statement.**

Although the concept of risk appetite looks simple and straight forward from the definition, in practice, it is very challenging to develop and apply an appropriate risk appetite statement.

The COSO framework provides guidance on developing a risk appetite framework. However, one important thing to note is that, a risk appetite framework must be organization–specific, tailored to the risks and culture of the organization– there is no one–size–fits all.

Nonetheless, I believe the following steps are critical in developing an appropriate risk appetite statement:

- Understand the organizational context [Mandate, objectives, political, economic, social, technological, and legal and regulatory factors, internal processes and systems, as well as stakeholder interests and influences].
- Assess the nature and level of risks the organization faces.
- Determine the level and nature of risks that you want to pursue.
- Develop a risk appetite statement and risk tolerance limits.
- Communicate the statement to the relevant stakeholders.
- Monitor compliance with the risk appetite.
- Review the risk appetite statement regularly.

**Conclusion**

A risk appetite framework is a fundamental tool in risk management, because it does not only ensure prudent decision–making by defining the boundaries of decision–making, it minimizes uncertainty and increases the chances of attaining organizational objectives.

# HOW TO STAY ON TOP OF OPERATIONAL RISK

***JOSHUA KIBIRIGE***
***Anti Money laundering Manager,***
*MBA, BCOM, CPA, CERM, PODITRA*

The Basel Committee on Banking Supervision (BCBS) defined operational risk as the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. Such risks include, poor customer service, human error, financial crime, staff turnover, business disruption, penalties or sanctions, system downtime, etc.

The practice of operational risk is relatively new, compared to financial risk management, and it is still abstract to many. For example, in banking, operational risk was elevated by the Basel Committee on Banking in September 1998 to become a distinct risk category. The position was reinforced after the financial crisis of 2008–2009.

Despite early adoption of operational risk management by financial institutions, many organizations are still facing challenges in implementing the practice. Failure or weaknesses in operational risk management can result into losses for organizations irrespective of size. For example, some companies such as the ones below, posted operational losses in June 2021, according to ORX news;

- Deutsche Bank lost $121.8 million in customer compensation, resulting from a fee increase ruling.

- Robinhood Markets lost $ 70 million for misleading customers and supervisory failures.

Operational risk is more complex compared to financial risk because, firstly, it is hard to measure, secondly, it often results in other risks e.g., if systems fail (operational risk), submission of tax returns could be delayed, thus resulting in penalties for non–compliance with the tax law. Thirdly, it requires having adequate visibility of all the processes within the organization, which creates a significant challenge.

The current changes in business models for many organizations, resulting from increased reliance on technology such as big data, artificial intelligence and machine learning, are generating demands on the operational risk management activities, which include using the existing data sets as leading indicators to make predictive analysis.

For organizations to stay on top of their risk landscape, they need to implement the following changes within their environment.

**1. Separate lines of defense**

The **first line** of defense includes personnel/staff who are involved in executing the day–to–day business operational activities of the organiza–tion.

The **second line** of defense includes risk management. Its key responsibility is to provide a proactive independent oversight to the first line of defense, through the following ways;

- Ensuring a mature risk culture is attained in the organization, where staff can anticipate opera–tional risks and report issues of concern.
The International Standard Organization (ISO 31000) defines risk culture as the system of values and behaviors present in an organization, which shape risk decisions of management and employees. A strong risk culture can help to mitigate exposures and to increase productivity.

- Timely risk monitoring and reporting. This can be done by putting in place predictive risk indicators, which give early warning signals before materialization of the risks.

- Ensuring a risk appetite is defined and communicated to staff, to guide decision–mak–ing within the organization. ISO 31000 defines a risk appetite as the amount and type of risk an organization is prepared to pursue, retain or take.

- Undertake organization–wide training and sensitization to enable employees to attain adequate understanding of the Enterprise Risk Management Framework (ERM)

The **third line** of defense consists of internal and external auditors. The third line of defense provides assurance on the effectiveness of risk management and the system of internal controls to those charged with the entity's governance.

The three lines of defense work coherently as a team, complementing each other's efforts in ensuring an effective risk management process, and in building a risk culture in the organization.

**2. Establish and regularly test the business continuity and disaster recovery plan**

Organizations need a business continuity plan (BCP) to ensure continuity of critical services of the business in case of a disastrous event. An effective BCP minimizes the impact of an unexpected event on business operations.

The ultimate aim of a disaster recovery plan is to minimize the Recovery Time Objective, which is the amount of time it takes a business to restore it's systems at an acceptable service level after a disaster. According to Touche Ross 2017, 90% of the companies that do not have a disaster recovery plan fail after a disaster.

**3. Align operational risk management to the performance of the organization**

Operational risk management should be at the core of organizational performance. The risks associated with the set goals and objectives of the organization should be identified and tracked along with the performance results. This means that key performance indicators (KPIs) and key risk indicators (KRIs) should be set at the same time.

KPIs are used in measuring the implementation of the company's strategy while KRIs are the main risk drivers, which provide early warning signals for risks that are emerging in the process of pursuing the strategic objectives. KRIs should therefore, be linked to the KPIs of the organiza–tion like in the example below;

| KPIs | KRIs |
|---|---|
| Employee retention | Number of Employee complaints |
| Reduction in IT system disruption | Number of unpatched IT systems |
| Customer satisfaction | Customer response time |
| Minimize loan defaults | Loans that exceed set credit limit |
| Revenue growth | Number of cancelled sales orders |

**4. Use data analytics to transform risk identification and analysis**

Organizations should leverage on the increase in data availability to employ data analytics in the process of risk identification and analysis. For example, due to the availability of big data, organizations can now integrate internal and external data when identifying emerging risks. This is done by compiling clear and up–to–date data sets that relate to a risk event being analyzed.

In conclusion, operational risk management should be treated as a core area within a business, not only to ensure survival during times of uncertainty but to also acquire a competitive advantage.




***MICHAEL SENDIWALA***
***Investment Risk Manager,***
*CFA, FCCA, CPA, BCOM*

# WHY UNDERSTANDING YOUR HUMAN AND FINANCIAL CAPITAL VOLATILITY IS IMPORTANT?

Human capital refers to the net present value of an individual's future expected labor income weighted by the probability of surviving to each future age, while financial capital are the financial assets accumulated by an individual over his or her lifetime.

The value of human capital is determined by several factors, both at micro (personal) and macro levels. At a micro level, an excellent education background often increases a person's human capital because it determines his/her starting salary. In addition, the size of the institution, the nature of the job or position, are key determinants of one's human capital. In many cases, initial salary varies based on vocation, nature of university and academic results, exposure and connections or family background.

At a macro level, human capital is determined by the level of a country's development. Citizens living in middle–income and advanced economies have higher human capital than those in low–income countries, because of higher earnings and longer life expectancy.

In addition, citizens in free market economies (capitalists) have better human capital than those in command economies. This is because, the payout is determined by forces of demand and supply, rather than being fixed by the state.

Human capital is a theoretical concept, which many do not live to realize fully. The biggest challenge for every individual is, therefore, to be able to convert human capital into financial capital. This is because the conversion process is not smooth and is mainly influenced by a number of factors, including:

**i) The growth rate of wage/ salaries**

This depends on the experience of the individual, level of inflation, nature of employer/industry, etc. For instance, the growth rate of salaries in the financial sector is, in most cases, greater than in the education sector, hence there is high human capital volatility in the financial industry than in the education sector.

**ii) Occupational income volatility**

The risks in job execution depend on the nature of the career; some careers are too risky because of the hazards associated with them, which can easily result in job loss or death. The higher the risks involved in job execution, the higher the volatility of human capital in that particular occupation. For example, occupations in a nuclear industry, offshore oil drilling rigs, chemical or defense industries and firefighting jobs, have greater human volatility than opportunities in other areas which are less risky, such as medicine, academia and public service.

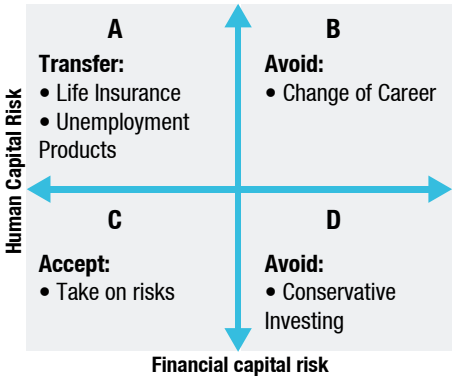
> " For an individual, it is important to match the volatility of human capital and financial capital to mitigate the risks associated with low financial assets at either retirement, loss of job or prema–ture loss of life"

**iii) Probability of survival**

This depends on several factors, which include but not limited to medical background and gender. For instance, a person with a poor medical background might not be in position to covert a reasonable percentage of human capital into financial capital, as compared to a person with a healthy medical background. The same applies to gender; females tend to have a high survival rate compared to the males; the global life expectancy for women is 74.2 years and for men is 69.8 years *(worldpopulationre–view.com).* This makes their (women's) human capital less volatile than that of men.

For an individual, it is important to match the volatil–ity of human capital and financial capital to mitigate the risks associated with low financial assets at either retirement, loss of job or premature loss of life.

Figure 1 below highlights the 4 quadrants, which can guide an individual on how to balance financial and human capital in order to avoid the pitfalls of limited savings at either retirement or death.




**Quadrant A: High HCV, Low FCV**

This represents an individual whose human capital volatility(HCV) is high, and financial capital volatili–ty(FCV) is low. Under this scenario, it is advisable that the individual invests in less volatile financial assets to ensure capital preservation, because the risk of losing his/her life or the job is high. In addition, he or she needs to get life insurance and unemployment insurance covers, because the risk of losing the job and life is high.

**Quadrant B: High HCV, High FCV**

Quadrant B represents an individual whose human capital and financial capital are very volatile (High Human Capital Volatility– HCV & High Financial Volatility– HFV), meaning that he or she has invested in highly volatile assets and he or she can easily lose his or her job.

This quadrant must be avoided at all costs because it is highly risky and susceptible to huge losses. For example, individuals in this quadrant who had invested 100% of their financial capital in subprime mortgages and stocks in the USA in 2008/9, might have lost all their assets during the global financial crisis, resulting into a nil net worth; and possibly they are now surviving on handouts. This quadrant has to be avoided because there is a high proba–bility for both human and financial capital to be eroded.

**Quadrant C: Low HCV, Low FCV**

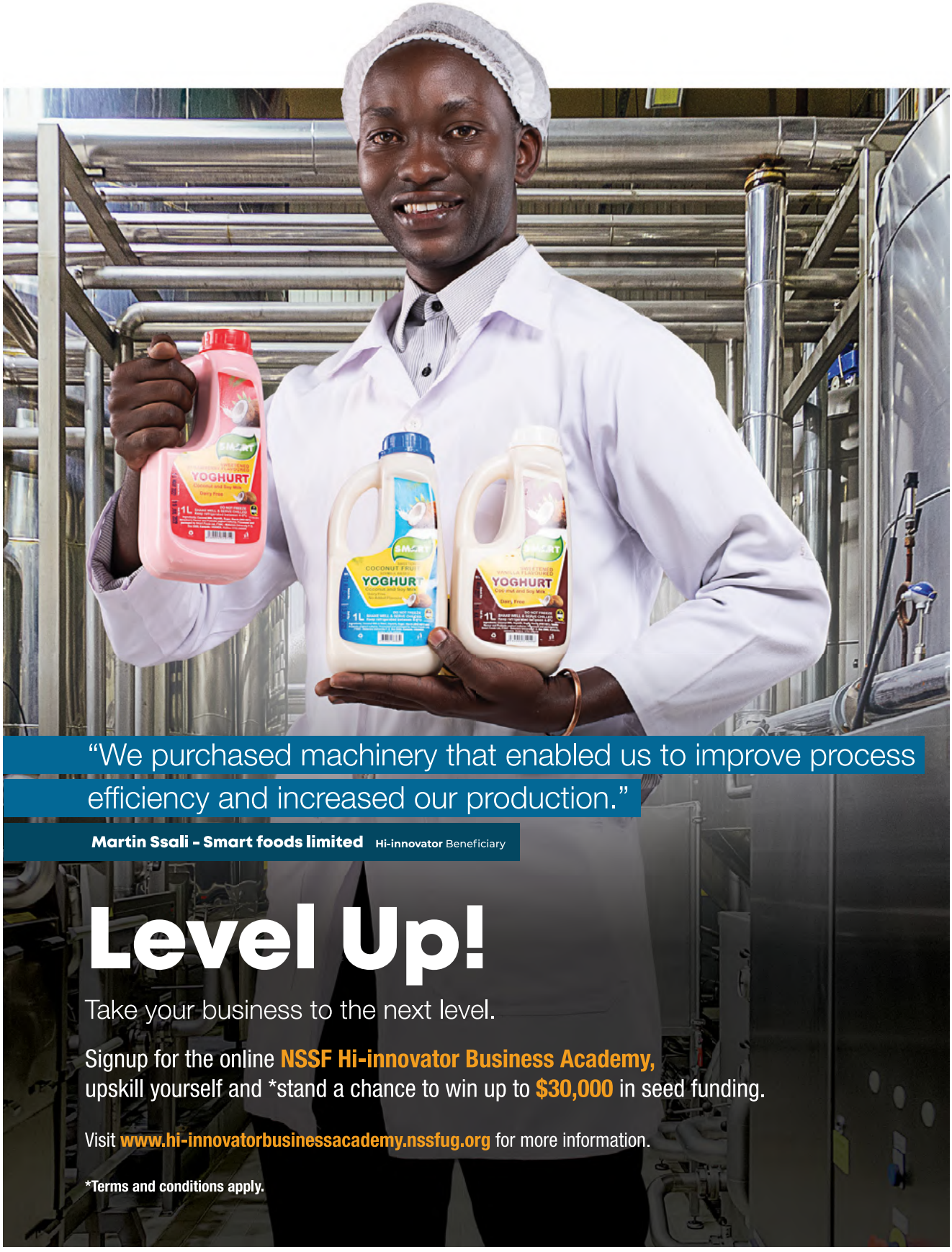
This represents an individual whose human and financial capital volatilities are low (Low Human Capital Volatility– Low HCV & Low Financial Volatility –Low FCV). It is advisable that such an individual takes on some financial risk even if his or her risk appetite is low. Investing in moderately risky assets can boast the growth in financial assets, since the possibility of losing human capital is low.

**Quadrant D: Low HCV, High FCV**

This quadrant represents an individual whose human capital volatility is low but financial capital volatility is high. This is a fair position because an individual can take on opportunities to exploit some gains from investing in risky assets given the low human capital volatility. However, it's important to align the investment strategy to the individual's risk appetite.

**Conclusion**

Understanding the nature of your human capital and it's potential implications on your financial capital can help you to reduce on human and financial capital losses.




"We purchased machinery that enabled us to improve process efficiency and increased our production."

**Martin Ssali - Smart foods limited** Hi-innovator Beneficiary

# Level Up!

Take your business to the next level.

Signup for the online **NSSF Hi-innovator Business Academy,** upskill yourself and *stand a chance to win up to **$30,000** in seed funding.

Visit **www.hi-innovatorbusinessacademy.nssfug.org** for more information.

***Terms and conditions apply.**

NSSF a better life | Hi INNOVATOR

Implementation Partner: atbox

In Partnership with: mastercard foundation | Young Africa Works

# ERM AND ORGANIZATIONAL PERFORMANCE AND GROWTH

***CYPRIAN MWESIGWA***
***Project Accountant,***
*MBA, BCom, ACCA, CPA*

An effective Enterprise Risk Management (ERM) framework involves an integrated approach of identifying, analyzing, assessing, quantifying, and managing risks of an organization, and it should form an integral part of the organization's strategic direction. The key objective of an ERM program is to reduce the uncer–tainties that can negatively affect the organization's operations, which in turn can affect its growth and financial performance. The benefits of a strong enterprise risk management framework include improved strategic and opera–tional decision–making, improved the organizations risk rating, in addition to improved business processes and the overall control environment.

The current macro and micro environ–mental uncertainties should trigger organizations to increase their investment in risk management practices, as they strive to achieve higher financial returns and growth. The uncertainties include but not limited to climate change, civil wars, external aggressions, and de–globalization, where countries are increasingly becoming more and more inward–looking, and in this respect we have seen countries come up with slogans like 'America first', "Buy Uganda Build Uganda" (BUBU), etc.

Consequently, organizations across all industry spectra should adopt an enterprise risk manage–ment framework that responds to the emerging risks if they are to stay afloat in this changing business environment.

While enterprise risk management is an important approach to managing dynamic and highly interdependent risks, the practical challenge that most organizations face is how to develop appro–priate programs for minimizing surprises, loss and costs, while enabling the organization to become more proactive, and balancing the tradeoff between investment in risk management and the return therefrom.

Many organizations find it challenging to realize the direct benefits of ERM and hence pay little or no attention to making meaningful investment in risk management, and this phenomenon is in part attributable to several reasons some of which are enumerated below.

**How ERM is perceived**

Many business leaders do not view risk management as an important integral part of the business processes and often do not attach the necessary attention to it. And because of this, the value derived from an effective risk management within the organization is not understood and yet without it everything can easily go to ashes.

**Resource commitment**

Risk management has generally been viewed as a cost centre rather than a value–adding activity, and because of that, resources required to implement all the necessary ERM initiatives to achieve the desired outcomes, are not allocated.

**Lack of Standard Measures**

Risks are not static; they evolve and change overtime and have no standard measures and benchmarks that different stakeholders within the organization can see and determine the value derived from effective risk management.

**Reporting**

Risk reporting sometimes is not standardized like other areas such as accounting and auditing, and often lacks or fails to capture the right metrics to trigger constructive conversations about the risk drivers.

**Risk management and Organizational Performance**

Risk management is often implicitly related to perfor–mance as it helps assess risks and develop strategies that can maximize organizational success. If risk management is done very well, it can enhance value creation and performance. By identifying issues that could negatively impact the business and devel–oping strategies to address them, implicitly contributes to the organization's performance. Some of the specific dimensions in which risk management contributes to organizational perfor–mance are discussed below;

**Risk management improves reputation**

Reputational risk arises from certain actions taking place within the company's establishment and if not managed well, they can lead to loss of financial capital, social capital and/or market share, result–ing in damage to a firm's reputation. Certain incidents that happen within the organization can cause the public to have a negative view of the organization.

If an organization has got a well–established risk management function, the fallout will greatly be minimized. When an incident inevitably happens, the risk management protocols will quickly contain the event and lower any chance of escalation of negative publicity.

It can be concluded that, managing reputational risk almost directly improves the firm's economic performance, in that, a good reputation increases market share, customer loyalty and retention.

**Catalyst for business success**

Risk management acts as an enabler for project success as it can reduce the likelihood and severi–ty of potential business risks by identifying and treating them early. If something goes wrong, there will be an existing guideline to respond to the problem. This helps management to prepare for the unexpected and maximize business outcomes.

It can, therefore, be concluded that effective risk management is a value–adding activity, which should be seen as an intangible asset. Business establishments that do not prioritize risk management take a lot of time undertaking corrective measures, long after many things have gone wrong. This does not only affect the company's reputation but can also erode business value.

**Risk management guides and improves decision–making.**

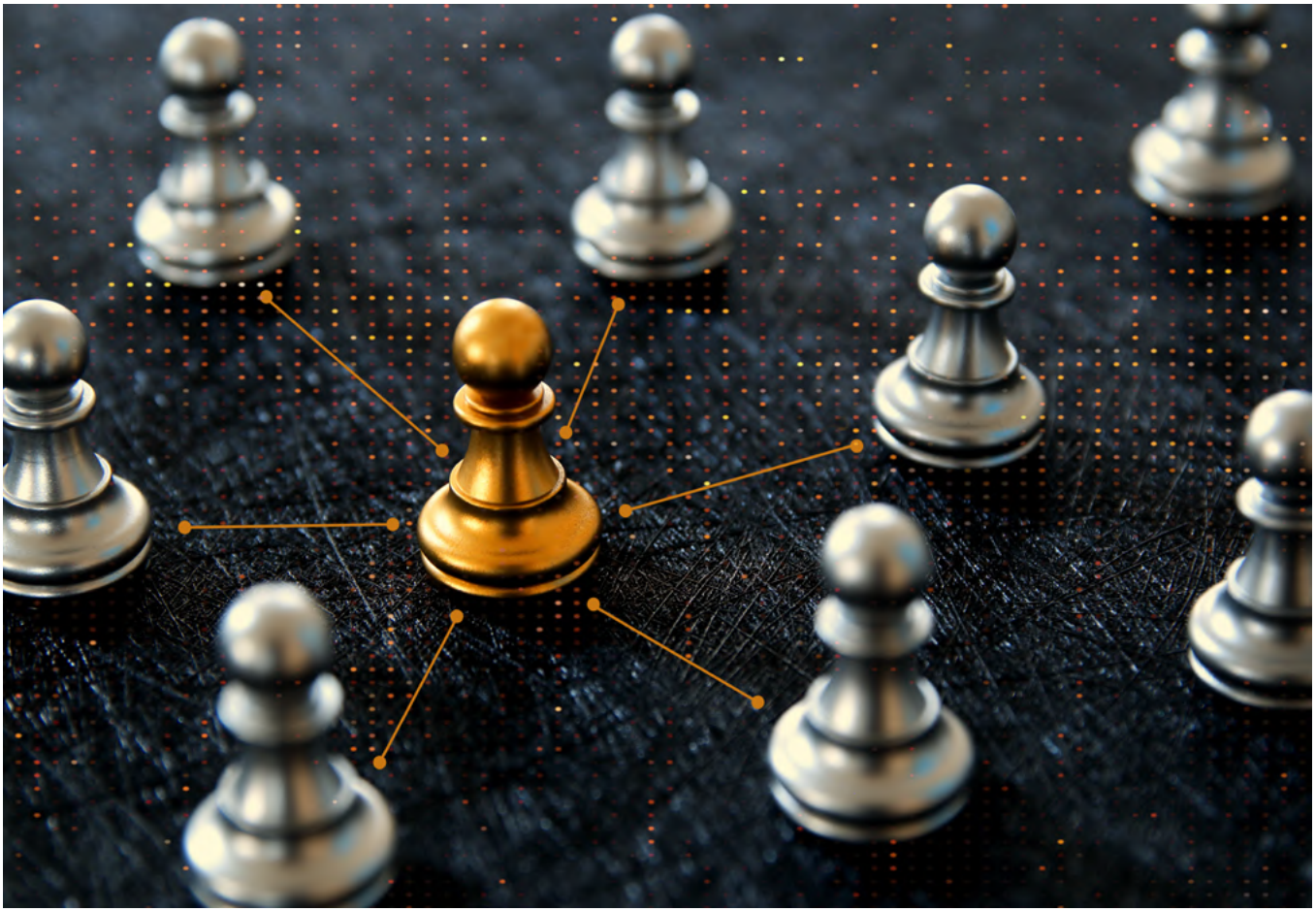
Decision–making can be a challenging process, especially when making choices that will have significant impacts on the future success of the business. Historical and current risk management metrics can guide manage–ment in making rational strategic decisions that will help meet or exceed the organizational set targets.

Tools like the risk appetite framework that defines the limits within which business decisions are taken, and the risk measurement matrix that measures the likelihood and impact of a risky event, are useful tools for decision–making. If the organization has got a robust risk function, it can guide on the strength and weaknesses of decision alternatives and provide recommendations on what risks to accept, transfer, pursue or avoid.

**Conclusion**

Managers, together with risk practitioners, need to focus on ensuring that all the elements of their ERM programs are appropriately integrated to ensure that they gain operational and strategic level benefits. As the business operating environment continues to be more dynamic and complex, there is need to increase risk management capabilities to counter the environmental challenges.

The changing business land scape, operational complexity and competitiveness will continue to increase and challenge organizations in ways they have never experienced before. ERM can provide a better pathway to improved business productivity, profitability and growth.



# INTEGRITY: A STRONG WEAPON AGAINST REPUTATION RISK.

***LAWRENCE SAKU***
***Financial Expert,***
*FCCA, CPA, BCOM*

Integrity is the quality or state of being complete or whole. It means being of sound moral principle. It is a ladder you keep climbing. Being a person of integrity implies honoring your word, a mark of an extraordinary leader. Integrity is a virtue that everybody would aspire to have but the unfortunate reality is that many fail the integrity test. The ultimate indicator of integrity is what you do when no one is seeing you.

Although integrity is about the inner being of a person, the environment in which the individual operates plays a big role in shaping the character and therefore, the integrity of the person. In the context of an organization, the bottom line is that the organization needs to walk the talk and let the tone set in the board room be communicated to everyone in the organization, both in words (oral/written), and in actions.

One of the revered investment gurus, Warren Buffet, once said that when searching for an employee, he focuses on three attributes; intelligence, energy, and integrity. If a person does not have the last quality, then do not bother with the first. Energy and intelligence without integrity is a recipe for disaster, as unethical behavior can cause financial loss and reputation damage. The rhetorical question however is, how do you objectively measure someone's level of integrity, especially at recruitment?

In the most recent case, which caused a lot of noise in the social media, some senior employees of Stanbic bank created a sham company, which they used to sell to themselves property belonging to a customer. The bank's reputation was affected, and it also incurred a financial loss when the commercial court condemned it to pay more than Shs400m as damages. This would have been avoided if these employees were people of integrity.

In an organizational context, integrity is reflected in the values, attitudes, beliefs, languages, and behavioral patterns within the organizational operating culture. Unethical practices involve the tacit, dishonest, corruption, fraud, and embezzlement of funds, inter alia. The situation can be worsened if top leadership doesn't fight these vices. They always percolate from the senior to the lower levels. If the senior executives are conducting business in an unethical manner, without following the policies and procedures in place, the junior staff will follow suit.

For example, the Uber 2017 scandal was allegedly caused by accusations regardingU ber's'bro' culture, which supported sexual abuse, and this was worsened by the allegations that senior members of the company had made sexist jokes and visited a brothel in Seoul. The scandal resulted in the resignation of the CEO, Travis Kalanick in June 2017. The company also had to make changes to its corporate culture in order to improve its reputation.

Companies which have maintained a good moral stand in society take deliberate steps to inculcate ethical values among their employees, and they do not stop at written values on websites or print outs on the walls, but they encourage their employees to live the values. Like I said earlier, building an ethical organization requires taking deliberate steps such as the ones below:

**Zero tolerance to integrity breaches**

Company policies must be tight and give no leeway to unethical behaviours, breach of which should automatically result in an exit of any member of the organization, no matter their seniority.
Mechanisms must be put in place to cater for reporting, and disciplinary measures in case an unethical matter is reported. The mechanism of reporting unethical behaviours must be known by everyone within and outside the organization, and should be confidential, independent, and fair to all parties involved. The process is more independent if it is operated by an external party, such as a law

firm, which reports directly to the Board rather than the CEO or any management committee. Ethical lapses by employees can put organizations at substantial risk. Although improved compliance with procedures can help limit this risk, successful efforts must extend beyond compliance to build a culture of organizational integrity.

**Live the core values.**

Many organizations have values, but they are just pinned on the walls; a few employees understand them, and the majority do not even bother to, at least, imitate a single element of them. The values have to be aligned to the purpose for the existence of the organization and must be reflected in the day–to–day activities.

The culture of ignoring the values of an organization is an indication of being untrue to the persona of the institution, and shows a lack of integrity.

Organizations have to make a deliberate effort to incorporate values in the operations. For example, quick quizzes about the values, and in–house competitions to educate staff about values, should consider which values are in play by making them a formal part of decision–making and performance appraisals. Staff have to be rewarded to the extent they exhibit and cherish the organization's values.

> "The journey to building a culture of high ethical standards that reflects in the day–to–day practices may be one of the most challenging approaches to building organizational integrity "

**Healthy organizational culture**

A healthy culture is one that cherishes doing the right thing no matter the cost. Sometimes an unethical practice appears to be rewarding, but in the long term, it is costly. For example, deliberately cheating customers or misleading regulators, can result in huge profits, like in the Volkswagen scandal, which resulted from the company's installation of a "defeat device" – or software – in diesel engines that could detect when they were being tested, changing the performance accordingly to improve results, caused a recall of 36,000 cars.
The implication of this was huge financial loss and serious reputation damage.

A strong organizational culture can mitigate the risk associated with gaps in the organizational integrity system because it helps to ensure that key values are incorporated into the working environment. The journey to building a culture of high ethical standards that reflects in the day–to–day practices may be one of the most challenging approaches to building organizational integrity, but the rewards are enormous; hence the organization has to take a deliberate effort to create a healthy organizational culture.

**A clear performance management approach**

The performance management system is a major source of integrity issues. If the performance measures are not clearly defined, it creates a culture of manipulation of results and encourages unethical practices. Unrealistic performance goals and pressure to achieve these goals at any cost sends a signal that ethical conduct is a low priority in the organization.

In additional, the way performance is managed in an organization can pose risks to organizational integrity, especially performance bonuses. Performance management bonuses can create perverse incentives to game the system in an effort to attain the targets. Therefore, it is necessary to be clear that success is not simply about achieving performance goals, but how they are achieved. This can be incorporated into performance reviews by including competencies related to standards of integrity.

**Conclusion**

Integrity plays a crucial role in ensuring sustainability and growth of the organization, as it helps to build trust among the organization's stakeholders, which is a key competitive advantage that leads to customer loyalty and retention.

# FAT – THE USEFUL BUT MISUNDERSTOOD NUTRIENT

***Dr. Paul Kasenene***
*Certified functional medicine practitioner, Nutrition expert & Wellness consultant, Managing Director, WellCare Ltd*

The issue of whether fats are good or bad for our health generates a lot of debate and can be quite confusing. Some experts tell us to limit or avoid fat altogether, yet others advise us to eat fat in large amounts. Well, what is the truth?

To address this issue, we need to understand; first, that fat is actually one of the macronutrients, which is a nutrient and not just some substance we find under our skin or in our body. Secondly, we need to recognize the fact that there are different types of fats, and that the different types play different roles in our bodies. But in principle, fats are designed to be largely beneficial for the body, although, due to specific properties of some of them, some can have undesirable effects on the body and even be unhealthy.

To understand this better, we can broadly categorize fats into two types, that is, saturated fats and unsaturated fats. Saturated fats are generally solid or easily solidify at room temperature, while unsaturated fats are mostly liquid at room temperature. For a long time, there has been a general belief that saturated fats are bad and that they cause heart disease and so should be avoided. At the same time, it was thought that unsaturated fats are better.

These statements are not totally accurate and can be misleading. Not all saturated fats are bad. For example, human breast milk has a fair amount of fat. A lot of it is saturated fat, which is beneficial to the body. Coconut oil and ghee are other types of foods high in saturated fat, which fat has been shown to be useful to our health because it reduces inflammation.

Indeed, some types of saturated fat may have unhealthy effects. Animals that have been reared commercially to grow rapidly and fatten quickly may contain a kind of saturated fat that can be linked to heart problems if we eat too much of it.

In addition, there is a type of saturated fat called transfats or hydrogenated fats found in marga–rine, vegetable shortening, and packed baked foods like biscuits and cookies that are extremely unhealthy and should be avoided. Transfats can block blood vessels and increase the risk for clots, strokes and heart attacks. So there are some good and bad saturated fats– not all of them are bad. There are also different types of unsaturated fats, including one type called monounsaturated fats.

**"Foods with a higher ratio of omega–3 and/or omega –6 fats are generally much healthier and should be eaten often.**

This is a very good and beneficial fat found in avocado, olives, almonds, cashews, chia and sesame seeds, and oils such as avocado and extra virgin olive oil. Monounsaturated fats help maintain healthy cholesterol levels, reduce body fat and help with weight loss. I advise that you often eat foods high in these fats. Another type of unsaturated fats is polyunsaturated fats.

These come in many types, but the most significant to note are omega–3 and omega–6 fats. Neither are bad. Omega–3 fats reduce inflammation and reduce blood clotting, while Omega–6 fats promote inflammation and blood clotting. Omega 6 fats are not necessarily bad because inflammation is an important response to injury in the body, and clotting is often useful to prevent excessive bleeding.

However, what is most important to keep in mind is the ratio of these fats in food. Foods with a higher ratio of omega–3 and/or omega–6 fats are gener–ally much healthier and should be eaten often.

These include chia and flax seeds, nuts such as walnuts, fish like salmon, as well as fish oils like cod liver oil. Omega–3 fats help remove fat from blood vessels and reduce the risk for blood clots and therefore, omega–3 rich foods are good for our health.

High concentration of omega–6 and/or omega–3 fats are usually found in cooking oils like sunflower oil, sunseed oil, safflower oil, peanut oil and corn oils. Because they have large amounts of omega–6 fats, they increase the risk for chronic inflammation and abnormal blood clotting. Such foods and foodstuffs that have a high risk of omega–6 and/or omega–3 fats should be avoided even if the fats are unsaturated and they are plant–based.

In conclusion, it is important to realize that not all fats are bad. Many are useful, and some are harmful. We need to get a good amount of healthy fats in our diet, while avoiding those that are unhealthy, with detrimental effects on our health.

I write in more detail about the issue of fats and in particular which oils to use and avoid, in my book entitled “Eat Your Way To Wellness”. You can get a copy at my clinic in Bugolobi or get more details on my website www.drkasenene.com.

***I wish you great health and wellness.***

# Dr. Kasenene

Food-Wellness-Renewal

VISIT OUR

# WELLNESS CLINIC

For a better and Healthier Lifestyle

## Food

Discover simple ways to learn about good nutrition and change your life forever.

## Wellness

Get a personalized health evaluation and understand your health risks.

## Renewal

Discover our unique wellness programs and begin your journey to great health today.

## Our Wellness Services

- Weight Management Program
- Detox Program
- Health Checkup & Screening
- Health Diet & Nutrition Services
- Health Boosters, Supplements, & Products
- Wellness Presentations
- Workplace Health & Wellness

## What We Manage

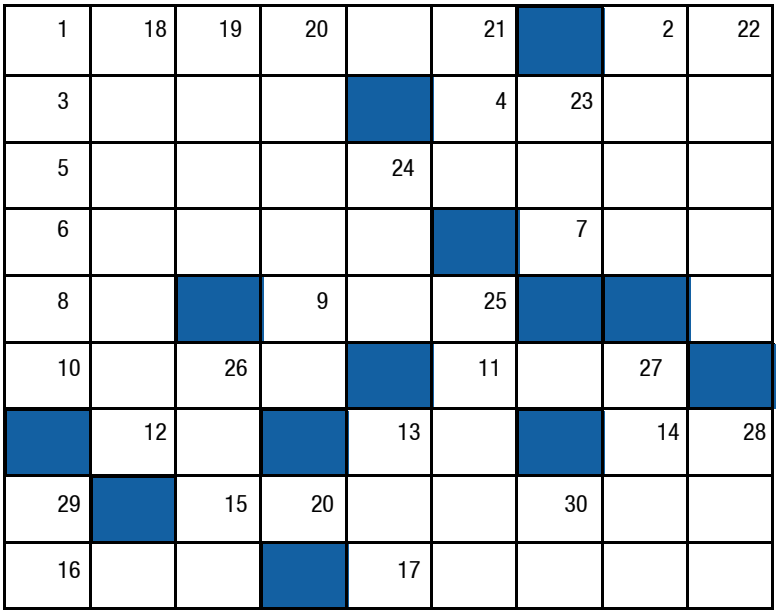
- Excessive Weight & Weight Problems
- Hypertension
- Diabetes
- Allergies and Asthma
- Arthritis
- Detoxification & Healing
- Digestive disorders
- Fatigue
- Heart Health
- Hormone Balance
- Migraines & Headaches
- Sleep and Insomnia

+256 701450450/ +256 761000 450

support@ wellcare.co.ug

drkasenene.com

# CROSSWORD PUZZLE: TEST YOUR KNOWLEDGE



**ACROSS**

**1.** Warning of specific limitations,6

**2.** Heads a police station, abbr.2

**3.** To a great or extreme degree,4

**4.** Brief written message or report,4

**5.** Got or brought back from somewhere,9

**6.** A seat without a back or arms, typically resting on say a single pedestal,5

**7.** Compass direction, abbr.3

**8.** (Suffix) forming nouns which were originally diminutives, 2

**9.** A measure of how efficiently a company turns sales into profits, abbr.3

**10.** (Lairs) Places where wild animals, especially fierce or dangerous ones, live,4

**11.** Security code for single–use, abbr.3

**12.** Execute, 2

**13.** Add (an amount of money) to an account, abbr.2

**14.** Working, 2

**15.** Approach, said of a person or time.7

**16.** Very good,3

**17.** Rubber coverings placed round wheels,5

**DOWN**

**1.** Uttered offensive words in anger or annoyance,6

**2.** An event regarded as a portent of good or evil,4

**13.** A pet with soft fur,3

**18.** Encouraged or assisted in doing wrong,7

**19.** A constitutional right to reject a decision or proposal made by a lawmaking body,4

**20.** Mistakes,6

**21.** Technical Matter Expert, abbr.3

**22.** A system of words, letters, figures, or symbols used to represent others, especially for the purposes of secrecy,5

**23.** The day immediately preceding an occasion,3

**24 .**International body devoted to promoting social justice, human and labour rights, abbr.3

**25.** Feeling sad or distressed through sympathy with someone else's misfortune,5

**26.** Not any,4

**27.** Unleavened maize bread in the form of flat oval cakes or loaves, 4

**28.** A sequencing technology that offers ultra–high throughput, scalability, and speed, abbr.3

**29.** Rated "very strong capacity to meet its financial commitments", by S&P Global,2

**30.** Of electromagnetic radiation, abbr.2

## Solution to Issue No. 4

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A | D | O | P | T | ■ | D | R | Y |
| M | O | P | ■ | A | I | R | ■ | E |
| E | N | T | E | R | ■ | M | I | S |
| N | ■ | E | X | I | T | ■ | L | ■ |
| ■ | S | D | ■ | F | O | I | L | S |
| L | C | ■ | ■ | F | I | T | ■ | E |
| U | A | T | ■ | ■ | L | ■ | M | T |
| C | R | I | S | I | S | ■ | E | U |
| K | E | E | P | S | ■ | O | T | P |

PAGE INTENTIONALLY LEFT BLANK

*A Full View of this Issue's Authors*


National Insurance