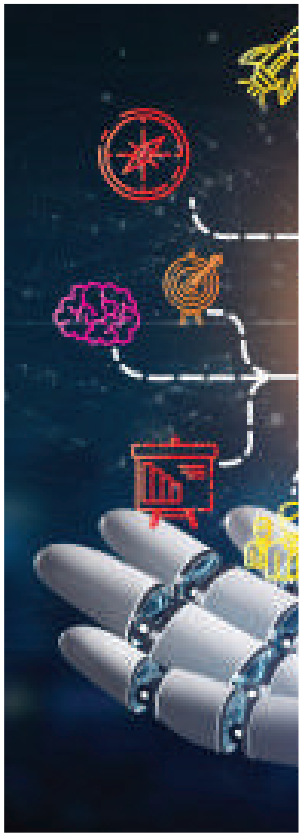
ISSUE TWO | DEC 2020

The RiskEcho

An Insightful Risk Management Publication by the NSSF

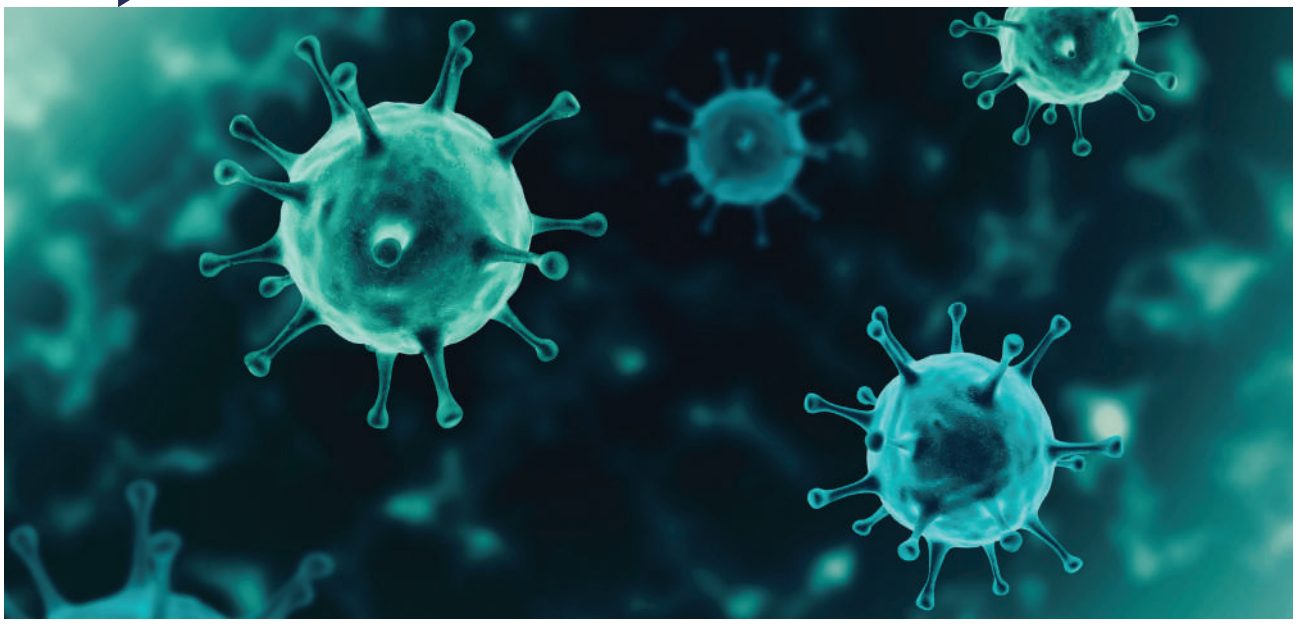
Inside

TABLE OF CONTENTS



FOREWORD

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



You are welcome to our second edition of The Risk Echo magazine. I am delighted to note that the first edition was warmly received by our readers. According to the survey conducted among the readers, the overall impression of the magazine was 94%. This was very impressive, especially given the fact that this was a pilot publication.

I take this opportunity to thank our readers for the feedback we received in form of comments, and we do pledge our commitment to implement the advice you gave us.

This edition comes at a time when the country is grappling with increasing cases of COVID–19 and deaths. As I wrote this article, 20th November, 2020, there were 17,148 confirmed cases and 158 deaths cumulatively, compared to 889 cases and zero deaths as at 30th June, 2020.

Unfortunately, there is high level of complacency in the country regarding the threat of COVID–19. Measures such as social distancing and wearing masks, that have been recommended by the Ministry Health in the fight against COVID, are hardly practiced. The political season has worsened complacency, as folks are too excited to think about COVID–19. A few who wear masks, pull them down when they need to speak, others wear them around their necks as if they were necklaces, exposing themselves and others to the virus.

The situation is even worse upcountry; where many believe there is no COVID–19 in Uganda, and others believe that COVID–19 is a Kampala problem.

From the time the first COVID–19 was detected 22nd March 2020, there was no COVID death until 23rd July 2020, following the easing the lockdown. This, coupled with mixed messages from some of the political leaders have created complacency among the population.

My simple advice to anyone reading this article, is that it is better to walk on the side of caution than to regret when it is too late– COVID–19 is real, COVID–19 is here, and currently there is no cure for it. The only solution for COVID–19 is prevention by adhering to the preventative measures recommended by the Ministry of Health.

On a lighter note, I am happy to bring you exciting topics in this edition such as Risk and return, a delicate balance, Resilience in turbulent times, Are defined benefits schemes booking their space in history.

Enjoy the reading.

Interview with the Deputy Managing Director of NSSF, Mr Patrick Ayota.

1. As a Deputy Managing Director, what role do you play in shaping the strategic direction of the Fund?

I have been supporting the Managing Director, in developing, coordinating and monitoring the implementation of the Fund's strategy.

2. You have been at the forefront of the Fund's innovation program. Briefly explain what this innovation program is all about?

We do recognize that there are so many opportunities that we have been given to bring additional value to both our members and Ugandans in general.

Given the constraints that we are all facing, the key is to figure out how to turn them into opportunities and create value as efficiently and effectively as possible. And that is when innovation kicks in. We have a group of very energetic and brilliant people, both within and outside the Fund. The issue for us was how to create an environment in which ideas can be birthed, nurtured, piloted and finally adopted as solutions to specific challenges. These ideas must create new products, improve access to our services by our members and other stakeholders, or make us more efficient in the delivery of services.

The largest Innovation program we have right now is to try to contribute towards solving the high unemployment rate that exists within the country. We have sourced some seed capital funds, for startup–business ideas that have the potential for impact, scalability and sustainability. We are procuring an idea management system to enhance our capability in running the Innovation program.

3. How is the innovation program aligned to the Fund's corporate strategy?

Our 10–year strategy, that we dubbed "Vision 2025", has 4 strategic objectives: Growth of the Fund to UGX 20Trillion, Efficient process with average benefit payment turnaround time of 24 hours, Engaged staff with a satisfaction rate of 95%, and wowed customers with satisfaction rate of 95%. The Innovation program is aimed at enhancing our capability to attain the above strategic objectives.

4. Innovation can be a costly venture; how do you intend to raise the necessary funds?

Innovation is indeed costly. However, what we have done is to leverage the Fund's resources, as well as partner with other key stakeholders to support the program. These include international partners with shared vision, such as Mastercard Foundation and local partners like, Outbox business services Uganda, and a number of banks.

5. Innovation is by trial and error, and the benefits may not be realized in the short term. How do you justify the cost involved?

One of the key requirements of innovation is that you must have the boldness to start, fail, learn, correct and try again. This process can be costly, but the benefits derived far exceed the costs incurred.

6. Since the Innovation program was launched in 2018, what would you say are the key achievements that have been registered so far?

The good news is that we have already seen the results of the Innovation program at the Fund. Innovations like the Ubiquity (anytime, anywhere), Straight Thru–Process and Self–service system features for our members, are some of the fruits of the Innovation program so far.

We have just completed a pilot program on our seed capital innovation and have funded 5 start–ups. We are monitoring the performance of these new entities.

7. Innovation is a "double–edged sword"; it can make or break you. How do you ensure that the down side is minimized, while taking advantage of the upside?

There are some prerequisites to minimizing the down side of the innovation activities.

At the Fund, we have embedded quality milestones at the various stages of the innovation process, and ensuring that from get go, there is a robust Risk register, that is regularly updated with new risks, and monitoring to ensure the implementation of the mitigations is done regularly.

8. Innovation is not an event that you plan to happen on a certain date. How then do you manage to have an innovation program?

The Board approved an Innovation policy, which has formalized the innovation process, together with supportive resources and structures.

We are slowly embedding the innovation culture across the Fund, from the Board, through the Managing Director, to Heads of departments and to all staff. We bring challenges to staff and celebrate innovations that come through.

9. Where do you see this program five years from now?

I am hoping that innovation will become Business–as–usual at the Fund. Out of this process, we will deliver products that bring optimal value to our members, and processes that augment the convenience value proposition to our members.

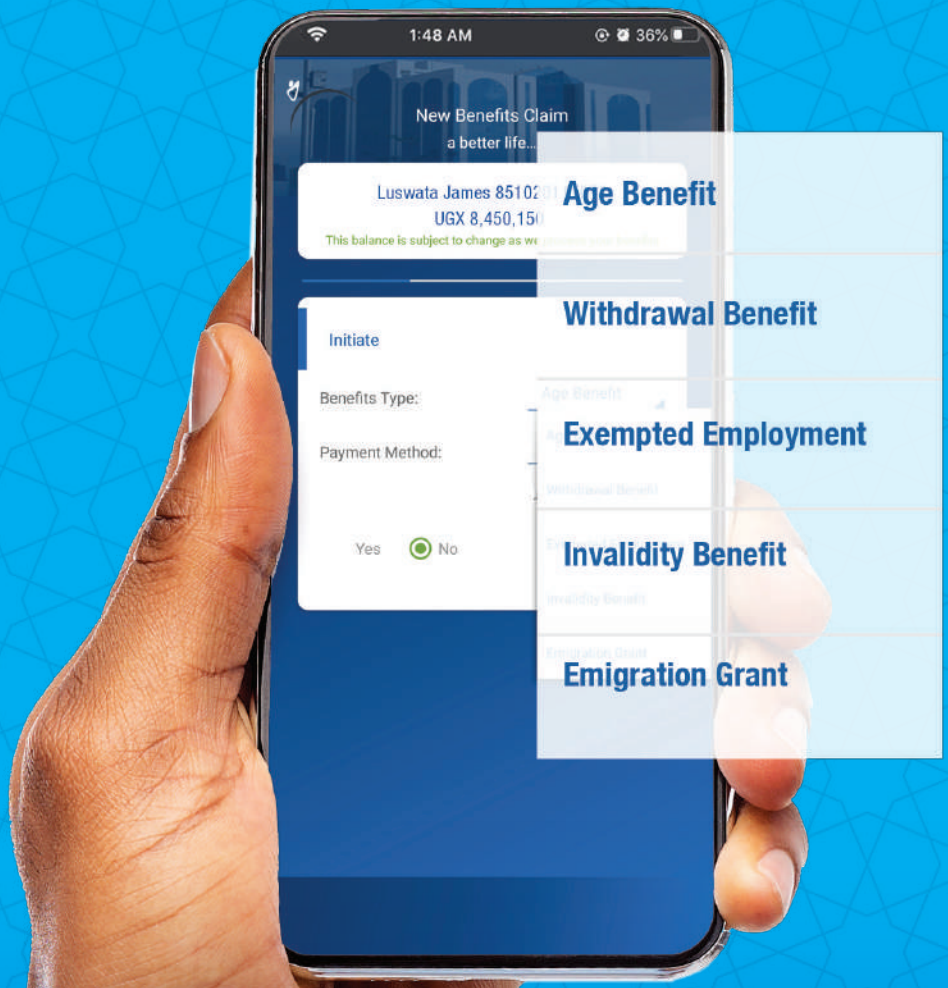
10. Any last comment(s) you would like to make to the readers of The Risk Echo?

I would like to encourage all companies out there, to create an environment in which creative energies of their people can thrive. The benefits will exceed the cost of doing so.

Queues

Skip the hassle

Submit your *benefits claim on the **NSSFGo App or NSSFGo Web.**



SCAN ME TO GET STARTED

*Applies only to qualifying Members'. For more information call **0800 286 773** toll free.

Download the **NSSFgo** app. Google play Visit **www.nssfgo.app**

NSSF
a better life

The Risk Manager's Dilemma

MICHEAL SENDIWALA
Investment Risk Manager,
National Social Security Fund
CFA, FCCA

A risk manager always encounters different dilemmas during the execution of his/her job but the ultimate need for understanding business needs, regulations/ laws and leveraging on his/her experience to deliver current and future value to the business, remains of great importance.

The risk manager's role has evolved from just being a coordinator of risks for the entire business (Guiding the front line staff on how to identify, mitigate and monitor risks) to becoming a risk advisor. The risk advisory role requires, a risk manager to offer practical solutions to the business. What organizations need, is not to stop projects but to focus on how to reduce the risk levels in certain projects (de–risk the projects).

However, the new role creates multiple dilemmas for a risk manager, which can undermine the effectiveness of risk management. For example, in the Wells Fargo scandal, where millions of unauthentic accounts were set up without customer consent, the accounts in some instances generated overdraft charges and other fees. This breach resulted into the firing of 5,300 employees, including the Chief Risk Officer.

The risk manager's role has evolved from just being a coordinator of risks for the entire business (Guiding the front line staff on how to identify, mitigate and monitor risks) to becoming a risk advisor.

However, the CEO claimed that he had no knowledge of this employees' activity; he was later forced to resign as the pressure increased.

The key question is, was the organization justified to fire the Chief Risk Officer?

This question reveals the dilemmas that the risk manager faces from time to time as explained below;

1. Expectation gap.

There is a misconception or an expectation gap that the risk manager knows or has to know all the risks facing the business. But in reality, can anyone know all the current and potential risks an entity is exposed to? Obviously, this is not possible, because no one, except God has the capability to predict the future with certainty.

Due to the expectation gap, if there are no risks crystalizing, everyone wonders what the risk manager is doing, and when things go wrong, they also question where the risk manager was. All these stem from the difference between what others think the risk manager is supposed to do and what he/she does as per the risk management practices.

Unlike other professions such as accounting, there are no specific standards for many aspects of risk management– this is left to personal judgement. Therefore, as a risk manager, you do not have to feel guilty that you were not able to "predict" the crystallization of a certain risk at an early stage, for instance COVID–19.

To address this misconception or expectation gap, as a risk manager, you have to create a culture, where everybody appreciates that risk management is a collective responsibility, and risk is part and parcel of the issues every individual has to deal with on a daily basis.

This requires undertaking continuous training and sensitization for all employees, highlighting the roles and responsibilities of each employee, and most importantly emphasizing the fact that everyone in the organization is a "risk manager". Every activity is associated with innumerable risks, and whoever is required to execute that activity, is also required to manage the associated risks.

2. Conflict of opinions.

A situation may arise, where in the opinion of a risk manager, a certain risk is significant and needs to be escalated to the Board, and on the other hand, the Chief Executive (CEO) thinks otherwise. But for the report to be submitted to the Board, it has to be sanctioned by the CEO. This situation, which emanates from the dual reporting structure, creates a dilemma for the risk manager, and sometimes causes the risk manager to water down the report to satisfy the desires of his boss (CEO). This can undermine the integrity of the report and may result in wrong decision–making by the board, as far as risk management is concerned.

To minimize this conflict, it is important that a standard criterion for what constitutes material risks to be escalated to the board is established. Such a criterion should define what is High, Medium or Low risk. High and medium risks should be reported to the executive management, and only high risk should be escalated to the board. All risks, whether low, medium or high, should be discussed at the functional/departmental/ division level before escalation to executive management and the board.

3. Complexity of operations.

Some organizations undertake complex processes such as chemical engineering, pharmaceutical manufacturing, aerospace engineering, which the risk manager may not understand well, hence failing to advise management on how to effectively manage the related risks. This coupled with the expectation gap, creates a big dilemma for the risk manager.

However, the risk manager does not have to be an expert in all fields, what he/she needs to do is to obtain a general understanding of the process and try to figure out what can go wrong or what opportunities can be exploited to improve the processes or add value to the organization. That means working closely with the teams involved in the processes, systems or products that the risk manager is dealing with.

Conclusion;

As a risk manager, your major role is to focus on how to build a strong risk culture in the organization, where everyone appreciates the concept of risk management and understands their risk management roles. Clear reporting lines and relationships at all levels is very critical, and always remember you are the risk advisor to the business.

How AI Will Transform Risk Analysis and Elevate Corporate Decision–Making.

JOSHUA KIBIRIGE
Anti–Money Laundering Manager,
National Social Security Fund
MBA,BCOM, CPA, CERM, PODITRA, ISO 31000

Every day the prominence of Artificial Intelligence (AI) increases, by being at the forefront of innovation. Its possible opportunities and uses seem unlimited given the data sources available.

For example, in the banking industry, Artificial Intelligence is already helping risk management to lower operational, regulatory and compliance costs, by providing reliable credit scorings, which are used in credit decision–making. AI has for instance, aided Nordic KYC utility, a creation of five major Scandinavian banks, to fulfil their "know your customer" anti–money laundering obligations, by using a range of machine learning techniques.

AI involves use of tools or machines that simulate human intelligence, and are programmed to think like humans or mimic their actions. Such tools will help organizations to improve their customer engagement and achieve cost efficiencies. For instance, we continue to see more organizations, including the National Social Security Fund, deploying chat boots in customer service in order to improve their customer engagement.

The process of conducting risk assessments will also be faster and more accurate when using Artificial Intelligence, by adopting both financial and non–financial data. AI will also help risk management to conduct back–testing and stress testing, which are key processes in risk management.

AI and machine learning will help risk managers approach the identification of risk variables in a new way. It will allow risk managers to isolate innumerable risk factors and understand their relationships at a greater level of complexity. The availability of big data, arising from the credit rating agencies, social media and public databases, will make it easy to understand risk at an individual level as well as at industry level.

Across the different industries, massive computing power is going to be able to help risk managers to identify patterns and relationships in data more quickly. Without supervision, machine learning will help the risk managers to identify the "unknown unknowns". Risk managers are therefore about to enter an age of plenty in terms of data volume and risk factor analysis.

Given that AI is a new technology, there are challenges related to its adoption. Questions on reliability of its output, human impact and transparency of the assumptions /algorithms embedded, are beginning to emerge.

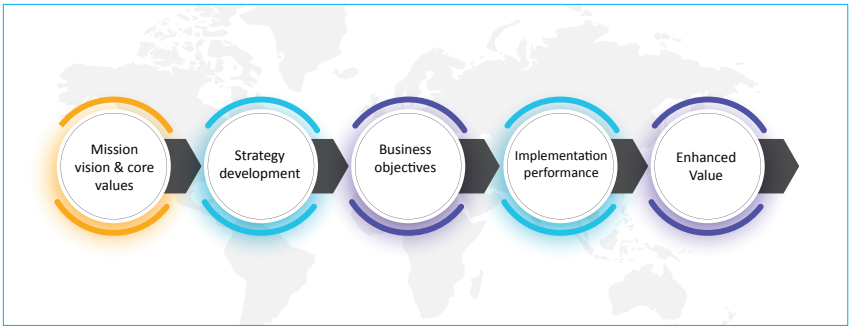
The solution to implementing AI in risk management lies in:

1. Embedding AI in your risk management framework

As organizations enter a new era of using Artificial Intelligence, it is important for enterprise risk management to consider the impact of such technologies on the organization.

It is therefore, relevant to include AI in a risk management framework, especially because it is a source of new risks and opportunities for the whole organization.

Adoption of the COSO 2017 framework can help to embed AI in enterprise management– See the diagram:



a) The first stage of vision and core values is determined by the Board of directors, who are supposed to set the tone from the top when adopting AI in the different processes of the organization. Management needs to advise the board about the importance of embedding AI in the organization's culture and processes.

The Board should also be sensitized on AI–related risks and skills requirements in order to guide their decision–making.

b) The second and third stage of strategy development involve including AI in the risk appetite. It also involves examining the value creation process of AI and understanding its impacts on processes, people and systems in the short, medium and long term.

In order to establish effective risk management processes and controls, any AI adoption strategy needs to align with the overall risk appetite from the start. For risk managers to be able to identify the threats, strengths, weakness and its opportunities, they should conduct a SWOT [Strengths, Weaknesses, Opportunities and Threats] analysis.

AI risk owners and IT teams should be involved at this stage to conduct a root cause analysis, which will help the risk managers to understand the risk drivers.

c) The Fourth stage of performance requires risk managers to identify risks associated with AI and to assess their severity and then implement controls to mitigate the risks. This process ends with communicating and reporting the impact of AI on the organizational strategy and objectives to the process owners.

Having done that, it is expected that risk management will improve, following the adoption AI, by automating some repetitive risk management steps, which will allow risk managers to allocate more time to new and emerging exposures within the business.

2. Human Impact

For organizations adopting AI, especially on a large scale, it will be essential to understand fully the impact that such transformation will have on their culture and talent strategy, and to put in place the necessary measures to address any adverse effects.

In all likelihood, the organization may need additional skilled technical resources to help design, test and manage AI applications. Developments in AI are expected to reduce aggregate demand for labour input into tasks that can be automated by means of pattern recognition.

Significant changes to employment practices, such as reduced staffing needs, or re–assignment of existing staff to different activities (with the associated re–training considerations), are likely to affect staff morale and, if not addressed promptly, may lead to an increase in unwanted staff turnover.

Excessive loss of personnel may jeopardize firms' ability to retain the necessary expertise and enough skilled staff able to perform processes manually if AI applications fail or must be retired at short notice. It may also have implications for the development of firms' next leadership generation.

Conclusion

AI will increasingly become a core component of many organizations' strategies to deliver better customer service, improve operational efficiency and compliance levels, as well as risk management, hence providing a competitive advantage to organizations that adopt it.

Are Defined Benefits Schemes Booking Their Space In History?

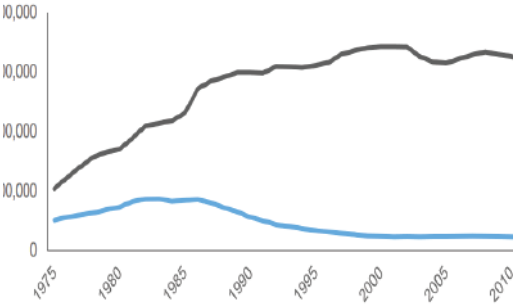
ROBERT MASIGA
Operational Risk Officer,
National Social Security Fund
BSTAT, CFA Level III

Unlike in the developed and middle–income countries, for most people in developing countries, Uganda inclusive, who live from hand–to–mouth, the issue of pension and retirement planning is a luxury, and worst still, many have never heard about the concept.

However, the history of pension funds can be traced far back over 370 years ago in 1645, by the then Duke Ernest, the pious of Gotha, a protestant prince, who decreed the creation of a fund to support widows of clergymen across his realm, according to Justin Owens, 2014.

Since then, pension systems have been evolving; from 1903 to 1950s, clear demarcations between defined benefits and defined contributions emerged. However, in early 1980s, preferences started shifting from defined benefits to defined contributions schemes– See the graph alongside that shows the number of schemes over time in the U.S

Figure 1 Defined benefit Vs Defined contribution



Source: https://russellinvestments.com

Defined contribution Schemes
Defined benefit schemes

According to Julia Kagan, 2020, a defined benefit pension scheme is a retirement plan, where the sponsor/employer guarantees retirement income determined by a pre–defined benefit formula for life, dependent on years the employee served the company. On the other hand, a defined contribution plan is an arrangement, where both

the employer and the employee contribute fixed proportions periodically into a fund that is paid out to the beneficiary as a lump–sum at retirement.

In Uganda, when one mentions a pension plan, what comes to mind is a scheme run by the government that guarantees post–employment benefits until someone's death, otherwise called annuities, for public servants. Other retirement schemes in the country operate on a defined contribution basis, the main one being the National Social Security Fund (NSSF). The NSSF covers employees in the private sector, non–governmental organization (NGOs) and semi–autonomous government entities, such as National Water & Sewerage Corporation (NWSC), Uganda Revenue Authority (URA), Uganda National Roads Authority (UNRA), the NSSF itself, etc.

The NSSF is a mandatory scheme, where each employee and employer are required to contribute 5% and 10% respectively, of the employee's monthly salary. In addition to the NSSF, there is one other mandatory scheme and 61 voluntary schemes, all operating on a defined contribution basis. Only four schemes in Uganda operate on defined benefit basis.

In developed countries, defined benefit schemes dominated until mid–1980s when many schemes realized that sustainability was becoming a very big issue. Indeed, the tide has been calm for the pension industry, where the employers and the employees have been sailing in the industry without major concerns.

It is of recent that employers, probably gave an eagle eye onto the bottom line of their financial statements and realized the need to shift the goal posts. Their choice is nothing else other than moving from defined benefits to defined contributions, and sooner than later, in the minds of many, corporate defined benefit (DB) plans are on their way to being part of history. This is very eminent even in Uganda, where, as I wrote this article, the government had tabled a bill seeking to repeal public pension and replace it with a defined contribution one.

The question then is, what is driving pension funds drifting from defined benefits to defined contributions?

Running either of the plans still requires managing risks but to a greater extent, the level of risks managed by a defined benefit sponsor are without doubt huge in terms of liquidity and sustainability.

Liquidity is a serious risk for defined benefits schemes, where complex models must be employed, like liability driven investing; involving strategies like interest rate immunization. Whichever the case, cash flows must be projected by the sponsor to meet the demands of the retirees.

Of course, this involves a lot of assumptions on interest rates and/or return, and asset classes that constitute the portfolio. And should there be any short fall, the employer/sponsor is obliged to fund the gap. The investment risk is borne by the sponsor, unlike in the defined contribution scheme.

This, in the process causes the health of the company's balance sheet to always be in check, which often raises eyebrows for the rating agencies.

This is mainly attributable to the longevity risk, where a pensioner lives longer than what the sponsor had anticipated, and therefore, the latter must pay extra pensions to the pensioner. This creates a funding gap for the sponsor and puts pressure on his cash flows.

World over, health services are improving, save for the recent disruption caused by the covid–19 pandemic. The general improvement, however, has led to improved health conditions, thus people living longer than initially projected, which creates a huge funding gap for pension schemes. Imagine an employee retiring at age 60 and lives up to over 90 years yet the benefits were projected to cover say 20 years after retirement! The 10 year–burden is shouldered by the plan sponsor.

Part of the financial crisis in Greece in 2009, as reported by Kimberly Amadeo, was due to longevity risk and the lavish pension benefits provided to pensioners. Of course, if the company (sponsor) does not have a strong financial base, chances are high that it can run out of business.

The public sector in Uganda is grappling with this problem, resulting in budgetary deficits. The Daily Monitor of 24th, September 2020 reported the need by the Ugandan government to provide for over UGX 10 trillion to satisfactorily settle the pension budget. This has a bearing on the country's ability to access debt visa–a–vis it's costs.

The current trend of defined benefits migrating to defined contributions has led to a high appetite to close defined benefit and transition to defined contribution, which has been the point of discussion.

In a defined contribution plan, once the plan participants contribute their fixed proportions, the funds are invested and whatever accumulates is paid as a lumpsum to the qualifying member, which marks the end of the relationship. Thus, in one way or the other, the risk of the retirement package not being enough to cater for the members' retirement life is entirely in their hands, depending on what they contributed and the investment they choose thereafter.

In conclusion therefore, although the initial framers of defined benefit schemes had good intentions of ensuring that the retirees live a financially stable life after retirement, little did they know that longevity would cause a serious problem to the pension schemes, to the extent of causing their collapse due to financial unsustainability. It is, therefore, not surprising that the current trend is more inclined towards defined contribution schemes.

Resilience in Turbulent Times

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

Before the onslaught of COVID–19, the issues of business continuity and disaster recovery were never thought about seriously in this part of the world, except as a waste of time and resources.

Most human beings tend to look at the past and the present in order to predict the future. For as long as something has never happened in the past, many will never believe it will happen. It is not common to find organizations conducting stress testing and scenario analysis to assess unlikely but plausible events, and to determine their impact on the business.

Interestingly, COVID–19 has overturned the tables and shown us that anything can happen. Prior to December 2019, nobody ever imagined that a disease like COVID–19 would break out and bring even the super powers to their knees, as well as lock down the entire world.

According to the Bank of Uganda, in 2019/2020, the economy grew by 3.2%, down from a projection of 5.4%. Several businesses have run bankrupt, and unemployment is soaring.

However, it is also true that there are many businesses that have remained resilient despite the widespread effects of the COVID–19, especially the lockdown imposed by various countries. Such businesses were able to make arrangement for their employees to work remotely and customers to access their services online. This demonstrates resilience.

That is as far as connectivity to the organization's internal systems is concerned. However, the big question to ask is, what if the organization's data center is completely destroyed? How many organizations in the country have built capability to recover their data in case the primary data is lost? My guess is that they are a handful.

Although no form of preparedness can completely eliminate a disaster, the ill–prepared will be significantly affected in case of a disastrous event. The best way to minimize the effect of a potential disaster is to have a comprehensive business continuity management (BCM) and disaster recovery plan (DRP)

The plan should be a five–stage framework, that covers the:

- Pre–incident phase
- Crisis management phase
- Disaster recovery phase
- Business resumption
- Post–incident evaluation

During the pre–incident stage, necessary infrastructure such the Business Continuity Management (BCM) & Disaster Recovery Plan (DRP) frameworks, Disaster recovery site and alternate sites, are established. The BCM and DRP governance structures are set up, and a business impact analysis (BIA) is conducted to assess the impact to mission–critical processes, in case of a disruptive incident.

A BIA is a systematic process for assessing the potential effects of an interruption to critical business processes. The BIA helps to identify potential disaster scenarios and strategies to prevent them from happening or to minimize the impact, as well as mechanisms to recover critical business processes in case a disruptive incident occurs.

In the BIA, recovery time objectives (RTO) and recovery point objective (RPO) are established. RTO is the time set for recovery of IT infrastructure and services, while RPO is the

maximum tolerable period within which data can be lost. The more urgent/ critical a system is, the lower the RTO.

The RTOs and RPOs are very important concepts because they are key determinants of the recovery strategy. If the organization desires low RPO, it must ensure data is frequently backed up or it has to invest in real time replication of data. Similarly, to have low RTO, the organization must invest in strengthening its recovery capabilities to minimize downtime, following a disruptive incident.

The BIA also helps to identify mission–critical or urgent processes, which must be recovered in the shortest time possible.

A crisis communication strategy needs to be developed in advance, which spells out how to deal with internal and external communication in a crisis mode. System recovery procedures are also documented and the IT recovery team is identified, and their roles and responsibilities are outlined in the DRP.

The other crucial aspects of the BCM/ DRP are the awareness and testing of the plan. If the stakeholders are not made aware of the plan, then it is likely that when the disaster occurs, they will not be able to follow the prescribed procedures in the BCM/DRP. Most importantly, the BC/DR plan has to be tested to assess its effectiveness.

When the disaster strikes, the BCM/DRP is activated. The criteria for invocation of the BCM/DRP needs to be set in advance. It is not every time an incident occurs that the BCM/DRP is activated. Activation of the BCM/DRP should be based on severity of the incident; minor or moderate incidents should be managed under routine procedures.

In conclusion, therefore, effective management of a disaster starts with having a comprehensive business continuity and disaster recovery plan, which is well communicated to the stakeholders and regularly tested to evaluate its effectiveness.

Embedding a Risk Culture

ADOLF BAGUMA
Operational Risk Manager,
National Social Security
MBA, CPA, CERM

A number of corporate executives have often viewed risk management and the overall control environment with resentment; understandably so, because they look at a catalogue of controls and procedures as an impediment, spoiler or limitation to the pursuance of corporate objectives.

This is probably so, because risk control imposes certain rules against which business actions, strategies or plans have to be based and these rules appear to be too bureaucratic and they technically slow down the speed at which business decisions are executed.

Risk managers often grapple with functional leaders to make them appreciate and implement risk control measures that appear as obstacles to the pursuance of the business objectives in their respective jurisdictions. This is because, very few corporate leaders do put risk management at the fore of their agenda, forgetting that a company with an effective risk management framework will run business more smoothly than its peers that are without one.

Why Risk Management

The purpose of risk management is to identify potential problems before they occur, so that risk–handling activities may be planned and invoked as needed across all business functions to mitigate potential adverse impacts on business objectives. Business managers and all employees ought to understand that incorporating risk management as part of a business strategy can enhance performance.

Risk management minimizes the consequences of uncertainties that would otherwise negatively affect the achievement of business objectives, hence creating new competitive advantage to the organization.

Every business, irrespective of its nature, size, location or industry, naturally faces the risk of unexpected events that can potentially be harmful to its progress and cost money or in worst case scenario, lead to collapse of the business. Risk management is thus, a tool that allows organizations to prepare for unexpected events by minimizing the chances of risk factors from crystalizing into risks.

Risk management as an inevitable undertaking cannot be ignored, as it can reduce the likelihood and impact of potential risk drivers or factors, by identifying them early and employing appropriate measures to prevent them from occurring or if they did, their impact would be marginal. This means that if something goes wrong, there will be an action plan in place to manage it.

Corporate executives do not like surprises, especially when it has an organizational wide impact or when it can affect the entity's reputation and possibly the company's earnings. It is therefore, important that management provides adequate support, to risk managers to map out all potential risks and then ensure that those in charge of the different business activities or processes work to prevent or best manage them.

Although it might be impossible to think of all possible risk scenarios and address them, risk managers can help make undesirable surprises less likely and less severe if they do occur.

Where an Organizations has a well–established formal risk function, it can help to substantially decrease the likelihood of risks materializing before they are identified and addressed. Even when an incident inevitably occurs, there will be risk management controls to quickly respond and contain the situation. This lowers the possibility of escalation and minimizes the extent of negative consequences and their impact on the business

Continuous engagement

Another important factor that can improve risk management culture, is continuous stakeholder engagement– by risk and other compliance functions. However, this can only be effective if senior management supports these efforts. In this way, stakeholders will realize that risk management effort is done with the anointing of the entity's top leadership.

Open communications

Open communication is yet another important component for effective risk culture. This creates a platform where all stakeholders are able to express ideas to one another, and are comfortable talking openly and honestly about risk, using a common risk vocabulary that promotes shared understanding.

Risk management minimizes the consequences of uncertainties that would otherwise negatively affect the achievement of business objectives, hence creating new competitive advantage to the organization.

What needs to be done to improve positive attitude towards Risk Management

Setting the tone at the top

The 'right tone at the top' is an important factor in enhancing risk management appreciation by everyone in the organisation. This could include holding all functional heads accountable for the implementation of the agreed controls. The tone at the top is set at all levels of management and has a trickle–down effect on all employees. If the tone set by management upholds compliance with controls, all employees are more likely to follow suit.

Goal congruency

All stakeholders within an organization should exhibit commonality of purpose: Employees' individual interests, values and ethics should be aligned with the organization's risk strategy, appetite, tolerance and approach. This view is also supported by Deloitte in their Risk & Compliance Journal of 2013

Universal adoption and application:

Risk management should be considered in all activities, from strategic planning to the day–to–day operations in every business unit within the organization. This will help embed the risk culture to be part and parcel of every decision or undertaking in the Organization.

In conclusion, I cannot over emphasize the need for risk management. Those charged with governance, in whom the ultimate responsibility for creating a robust risk management framework lies, must view risk management as an enabler, and a priority worth an investment.

There are strong business reasons for having a robust risk management program. Companies should endeavor to place risk management at the fore of their activities, and not treat it as an afterthought.

Communicating The Cost Of Information Security Effectively.

STEPHEN BABIGUMIRA
Information Security Officer,
National Social Security Fund
Msc IS, CISSP, CRISC, CEH, CISA, ISO 27001 LA

One evening when I was about to close off my day, I received a call from an information security specialist working with one of the commercial banks in town. He was in desperation for a response that would get him some relief from the bank's top executives.

Top management was asking the hard questions about information security budget. In particular, they wanted justification for the huge investment on information security tools. In addition, they wanted him to benchmark with my organization on what tools we had implemented. I was fast to list the tools we had implemented, and fortunately for him, my organization had implemented more tools than they had.

After I mentioned the tools we had acquired, I heard him breath a big sigh of relief like a prisoner who had been convicted of murder getting a pardon from the President. I guess he was smiling ear to ear and wanted to end the call having gotten the answer he wanted.

At the back of my mind, I knew what I had told him wasn't the appropriate ''answer'' the executives wanted to hear and he would face the same question over and over again.

To help him be prepared for such questions, I went ahead and told to him that due to the nature of my organization's business, the threat and risks we faced were quite different from what his organization faced; our risk appetite was not exactly the same as that of his company. Therefore, the investments in security could not match tool for tool or penny for penny. "Oh yeah, now I get it", he retorted

It is important to note that such situations are not unique to my friend and his organization; many security managers will tell you similar stories.

But why is that a number of executives are reluctant to invest substantially in information security? Part of the reason is lack of direct correlation between investment in security and the bottom line. For many executives, something that does not directly impact the bottom line is not a priority.

Although some executives may be interested in protecting their information assets against

any breach and are willing to splash the budget, they also have the same appetite for accounting for every penny they authorize to be spent.

Secondly, and probably the most critical reason for the reluctance to investment in security, is lack of awareness of the nature and level of exposure to the organization. According to a research report (2016 Outlook: Vulnerability risk management & remedial trends), by Nopsec, over 60% of 200 participants in a survey stated that their executives were "somewhat" or "not at all" informed about information security risk and the threat their organizations faced. In an era of high possibility of litigation due to data breach, lack of awareness of the risk exposure in itself is a major risk to any organization.

That said, it is important that the security manager develops a communication strategy to convincing the reluctant executives to spend substantially on information security, so as to protect the organization against litigation for data breach and reputation damage.

One way to effectively communicate your information security portfolio is to drive every investment in information security basing on the threats/risk your organization is facing. In other words, each information security control (which can be in terms of a tool, procedure) you are implementing, should be traceable or back to a particular risk.

The linkage between risk and expenditure helps the executives to appreciate why they need to spend what they need to spend. Lack of a proper linkage between expenditure and risk could put you in a situation where you are buying/using a 'gun to kill a mosquito", or buying/using a 'knife' to kill a lion".

Having an information security risk and control matrix will help ease the communication and understanding between the executives and the cyber security managers, which is normally curtailed by the difference in academic backgrounds and the love for use of technical jargons by the cyber security managers.

Secondly, the Cyber Defense Matrix (CDM) – see below developed by Sounil Yu, a renowned Chief security scientist, is a great tool that can help you have the right and timely answers in regards to the investments in information security tools. It will make it easy for you to talk about investment in information security.

The CDM is a five by five structured matrix that combines the security functions of the NIST Cyber Security Framework – Identify, Protect, Detect, Respond and Recover, as columns; with a set of commonly accepted asset classes – Devices, Applications, Networks, Data and Users as rows.

At the bottom of the grid, there is a continuum that symbolizes the degree of dependency on technology, people, and process, through the five operational functions of the NIST Cybersecurity Framework.

There is a consistent reliance on Process, a strong dependency on Technology solutions under Identify and Protect, and an increasing reliance on people, as you move towards Detect, Respond and Recover.

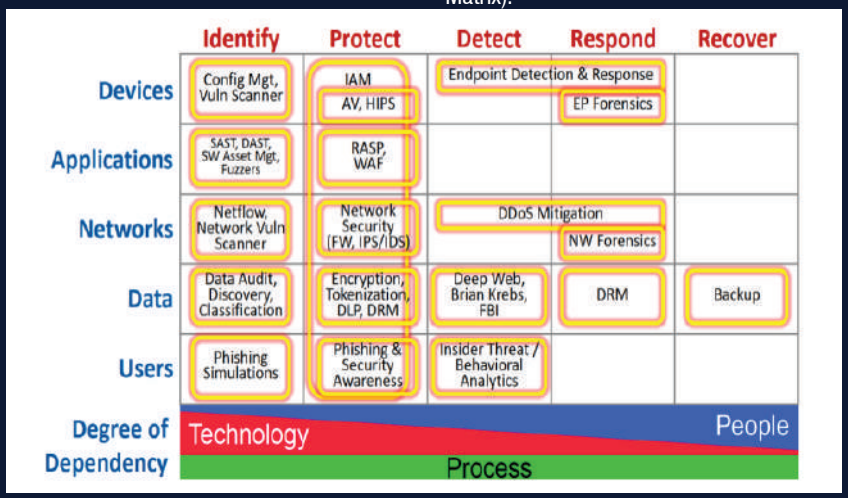
The "Identify" and "Protect" functions are used prior to a security event and the other three remaining functions i.e. "Detect", "Respond" and "Recover" are used after a security event.

This tool can be used to map, measure and justify the information security portfolio of your organization. The example of the matrix indicates the distribution of information security solutions

The visuals in the CDM help to identify the gaps in technology, people and processes, duplications and help you see where you have too much and you need to actually get rid of technologies.

Conclusion

Although many executives are less willing to spend on information security because of the apparent lack of correlation between information security and organization value, coupled with lack of clear understanding of security exposures, this situation can be turned around by better and effective communication strategies by the information security manager. Most importantly, the conversation should involve linking security expenditure to the level of threat, and employing tools such as CDM (Cyber Defense Matrix).



Risk and Return, A Delicate Balance

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

A return on investment is the main driving force behind entrepreneurship and business. Everyone who starts a business or an economic activity expects to receive a return; and the higher the expected return, the higher the propensity to invest, ceteris paribus. Anyone will tell you that an investment that doesn't provide a positive return is not worthy undertaking.

Return on investment is simply a financial ratio which indicates what the investor receives in relation to their investment cost. In other words, it is a relative gain on investment over the cost of investment.

$$\text{Return on investment (ROI)} = \frac{[\text{Investment revenue} - \text{Cost of investment}] \times 100}{\text{Cost of investment}}$$

Return on investment metrics such as return on equity (ROE), return on assets (ROA), return on capital employed (ROCE), etc., are key investment performance measures; the higher the metric, the higher the performance in terms of profitability.

Although the desire of every investor or entrepreneur is to get a positive return on investment, a positive return is extremely illusive, and it is not uncommon for an investment to realize a negative return– the question is why?

The reasons or factors that influence a return on investment are numerous but all of them can be summarized in a four–letter word called 'risk'. Although often times risk is not considered seriously because the focus is mainly on return, risk accounts for the majority of negative returns or investment failure. Risk is the most important factor determining the level of return on any investment. As a matter of fact, a return is a function of how the associated risk is managed. Risk and return are two faces of a coin; just like a coin has two faces, the two faces of an investment are the risk and return.

Although it is generally believed that investment in government securities such treasury bills and bonds is risk–free, as the investor is guaranteed a fixed return in form of a yield, the truth of the matter is that even such investments are not totally free of risk.

The default risk for example, is a possibility, though very remote. There are a number of examples of countries such as Argentina, Russia, Pakistan, etc, that defaulted on the payment of interest and principal on sovereign debt. Therefore, the possibility of a bond issuer failing to meet their obligations as they fall due, creates a risk to the bondholder.

Secondly, in times of war or violent take–over of a government, the return on investment in government securities may not be received in time, creating a liquidity risk on the side of the bondholder. Even the time value of money would be an issue in the circumstances.

The other equally important aspect that an investor needs to appreciate is, as the saying goes, the high the return, the higher the risk. Meaning that, if you want a high return, you should be willing to take a higher risk. High levels of risk can have a catastrophic impact on the returns if the risk is not well managed.

For instance, the source of the global financial crisis of 2008 can be traced from the desire by financial institutions to make huge profits. Through their innovative concept of debt securitization or "generate and distribute" concept, banks were able to make huge profits by generating loans, repackaging them and selling them to various investors.

The most common ones were the mortgage–backed securities (MBS).

An MBS is a type of asset–backed security, which is secured by a mortgage or a collection of mortgages. The mortgages are aggregated and sold to a group of individuals or government agency or an investment bank that securitizes, or packages them together into a security that investors buy [en.m.wikipedia.org].

The structure of the MBS may be termed as "pass–through", because interest and principal repayments from the borrowers or homebuyer pass through it to the MBS holder, or may be complex made up of other MBSs.

Traditionally, banks generate loans and maintain a portfolio of loans. Because they are concerned with credit risk, they do due diligence on the borrowers to assess their credit worthiness before disbursement of the loans, to minimize the risk of default. However, under the generate and distribute arrangement, the banks were able to transfer the credit risk to the investors by selling the loans to the investors. The repayment of the principal and interest went to the investors, and that meant the investor bore the credit risk. This arrangement was beneficial to the banks because the banks received immediate cash flow upon sale of the loans and were able to successfully transfer credit risk to the investors.

Orville Wright's famous first airplane flight, December 17, 1903.

This resulted in a situation where the banks became more aggressive in generating loans in pursuit of the lucrative market for MBSs, and in the process they relaxed controls on credit origination. This meant increased lending to subprime borrowers – borrowers of low credit worthiness. When interest rates increased in the US, the subprime borrowers could no longer afford to service their loans and began to default.

According to Mary Bellis (2019), many banks, especially those with exposure to subprime, experienced large loses and liquidity issues. Institutions became overly cautious, hoarding excess reserve and unwilling to lend to other cash–stricken institutions. Unfortunately, this was too little too late to avert the crisis, the rest is history.

Recall that it all started with someone seeking to earn a high return by the novel idea of MBSs, which was a complete departure from the traditional loan portfolio management, and in doing so, controls had to be relaxed because they were seen as obstacles for portfolio growth.

Of course that is not to say or imply that risk–taking is extremely dangerous and that it should be avoided, because that would mean giving up on investment and life, as every aspect of life involves an element of risk.

Value is created out of risk; one of the most important inventions of the 18th century was the invention of an airplane by two brothers, Orville and Wilbur Wright. Before their maiden flight in 1903, it was unheard of a human being flying in the air like a bird!

The Wrights took the greatest risk of their time and it paid off; today the plane is the most magnificent and elegant means of transport.

In conclusion, therefore, the point I am making is that as you pursue a return, remember that it is wrapped in uncertainty, whose outcome could undermine the very return you are pursuing.

It is therefore, important, as you pursue an investment opportunity, to seek to understand the nature and level of risk you are taking on, and establish appropriate risk mitigation strategies.

The Perils of Ineffective Risk Management Practices

ADOLF BAGUMA
Operational Risk Manager,
National Social Security
MBA, CPA, CERM

Many corporate entities, including those with global scale operations, have either collapsed or have come to the verge of collapse due to lapses in their risk management practices or philosophies.

It could be argued that some of these entities relied on the delusion of 'too big to fail', and along the way undertook miscalculated risks coupled with ineffective risk management models.

The unabated success of some corporate entities often entices them to take on any opportunity that comes their way without a clear understanding of the associated risks. This is in line with the research conducted by Bolton consulting Group (BCG), which revealed a significant relationship between revenue growth and mortality. 'Accelerated growth correlates with shorter life spans; whereas companies with more moderate growth face the lowest risk of collapse'

Let us now look at some of the giant corporations that have either collapsed or experienced significant financial losses due to ineffective risk management practices over the last decade or so and examine the reasons why they fell victim to their own successes and possibly pick a few lessons for our own sake.

Barings Bank

The failure of Barings bank, one of the oldest and richest bank of our time, sent shock waves across the corporate world, especially in the financial services industry. The bankruptcy and eventual closure was majorly on account of ineffective or failed risk management practices employed by the bank, where a young executive was allowed to execute unlimited trades in long positions at the Nikkei 225 futures, which resulted into phenomenal losses that were later concealed fraudulently for several months– Andrew Beattie (Investopedia.com editorial team)

The above facts are indicative of management's failure in determining the bank's risk appetite in respect to derivative trading segment of the portfolio and trusting an individual trader to manage huge volumes of positions (in billions of USD) unchecked. This was an obvious misstep in their risk management practices, which some industry experts termed as 'a risk management disaster'

JPMorgan Chase (JPM)

JPM is another giant which was once credited with having one of the most robust risk management practices in the financial industry. Despite having a keen focus on risk management, an inquiry into the USD 6 billion loss in 2012 concluded that risk management practices at the bank's Chief Investment Office (CIO), the business unit in which the loss occurred, were given less scrutiny by senior management, despite the fact that the Chief Investment Officer managed a colossal volume of assets to the tune of over USD350 billion– (https://elischolar.library.yale.edu/journal–of–financial–crises)

The JPM case appears similar to what I already mentioned in the Barings bank scenario, where an individual is given so much powers and control at the expense of internal control checks and prudence.

Crane Bank–Uganda

Getting closer home, a number of corporate giants have also fallen victim of risk management failures and the most recent causality being the former Crane Bank

At the time of its take–over by dfcu bank in January 2017, the bank was hither to one of the largest and most profitable financial institutions in the country, with well over UGX 1.8 trillion in assets, according to the Central Bank of Uganda (BOU). Crane Bank limited (CBL) was grossly undercapitalized and posed systemic risk to the Banking sector in Uganda.

Some of the causal factors for CBL's failure are no different from those of its peers already discussed in the text above –insider trading, related party dealings and miserable corporate governance practices coupled with regulatory non–compliance, according the BOU's arguments for placing the bank under receivership. All the aforesaid cases point to failed or inadequate risk management practices.

Lessons learned and mitigations

i) Risk Governance failures.

Failure in risk governance and discipline, resulting in corporate value creation and growth initiatives superseding the risk concerns and early warnings raised by the independent risk management and compliance functions.

Mitigation: Management ought to pay close attention to the trivialities of all risk indicators raised.

ii) Lack of risk tolerance limits.

From the above case studies, collapse of the banks was partly attributed to their failure of having approved tolerance limits that would ensure prudent risk–taking within the precincts set by the organization's risk appetite framework.

Mitigation: Organizations should always endeavor to have risk tolerance limits approved by those charged with governance, which explicitly defines the limits within which each business undertaking is conducted.

iii) Failure to integrate risk management with strategy–setting

The culture in an organization where risk is treated as peripheral to strategy–setting, may result in having strategic objectives that may be unrealistic and risk management becoming an adjunct to performance management. The consequences of this mismatch could be dire, including failure to achieve the organizational objectives, erosion of enterprise value, and sometimes the demise of the entire enterprise altogether.

Mitigation: In as much as practicable strategy setting should be integrated with risk management to ensure that the strategy is being pursued in line with the risk appetite and capacity.

iv) Lack of effective risk assessments

Risk management failures could also be caused by risk assessment mechanisms, which are not identifying the critical business risks effectively, efficiently and promptly. Or at worst, no risk assessment is conducted regularly.

Mitigation: With the dynamic business environment, business enterprises should periodically, as defined by the board, review and bring up–to–date the risk profiles of all the business units under management.

Conclusion

While some corporate executives have placed more emphasis on growth and profitability, they often forget that the business operating landscape has overtime become increasingly unpredictable and therefore they need to pay closer attention to risk management, lest they face similar calamities that befell the above mentioned giants.

Senior executives should recognize that the future is inherently uncertain and the business environment is too complex for anyone to predict with certainty and hence the need to have an eagle's eye on potential risks that can negatively affect the achievement of their strategic objectives.

www.nssfug.org /nssfug nssfug 0800286773 TOLL – FREE

NSSF e-CHANNELS

easy | instant

Tap into the world of convenience

All our services are online.
No need to visit any of our branches.

#NssfOnTheGo

SMS
6773

NSSFGo App

Web
nssfug.org

Web App
nssfgo.app

USSD
*254#

Toll Free Line
0800286773
0784259713

NSSF
a better life


N.S.S.F PENSION TOWERS
PENSION MALL

Trust And Estate Planning: An Effective Model for Estate Management

ROBERT MASIGA
Operational Risk Officer
National Social Security Fund
BSTAT, CFA Level III

In Uganda, estate management, which entails preparation of the tasks that serve to preserve, manage, and distribute an individual's asset base to the beneficiaries, in the event of the former's incapacitation or death, is still a grey area and thus not given the due attention.

Every other day, we still come across news of families fighting, including killing each other over property left by their deceased relatives. In my early twenties, there was a prosperous family in my neighborhood that I admired. The husband had a well–paying job, the family lived in a luxurious house, and the children went to expensive schools. It was a kind of family many would consider very successful. Unfortunately, the husband died in a motor accident, and left no will. From that time on, the wife and the children's lives changed forever and for worse. The relatives started grabbing the deceased's property and threw the wife out of her matrimonial house. Unfortunately, this is not unique to my deceased neighbor's wife; often times, many families have been left desperate, as relatives scramble for the deceased's property.

Surprisingly, this continues to happen despite the existence of the succession Act of 1906. Although the law is not up to date, having been enacted so long ago, it clearly outlines the distribution of the deceased's estate.

This unfortunate reality, implies that, many Ugandans have not yet learnt to plan for the management of their estates after they have departed. This could be attributed to cultural sentiments, beliefs/ practices or simply ignorance of the available alternatives that would otherwise be more effective. For instance, in many cultures in Uganda, people believe that making a will is a curse or an invitation for death; and yet a will helps to distribute the assets of the deceased in accordance with the wishes of the deceased, which minimalizes scenarios such as the one described above, that befell my deceased neighbor's wife.

The aforesaid alternative includes, but is not limited to obtaining a revocable or living trust that allows you to maintain full legal control and ownership of the trust, including the properties and assets, until the time of your death. This means you can add/remove assets or properties anytime you want, change beneficiaries, and even dissolve the whole arrangement should your situation change.

This further supports the argument that, much as no one would wish to be

incapacitated or to die; planning in advance for the bequest is the ultimate solution to many of the issues that come up after the unexpected event unfolds. It is with no doubt that many parents toil to secure a better future for their family members, especially the children and the spouse, in terms of education and social welfare. But it is very painful to see them (children and spouse) become paupers or vagabonds on streets if not in villages, when their parents' or spouse's wealth is put to waste or lands into wrong hands of those who purport to have secured rights to be administrators of the deceased's estate.

Time therefore, has evolved, where the need to rise to the occasion and live within the existing reality is high. This necessitates doing the needful and preparing for undesirable but realistic occurrence, by having the mitigants put in place.

With the growing number of financial services globally, estate planning and management can effectively be executed through several tools. However, in this article, I will focus on a trust and how it works.

The Trust and how it works

A trust, being the most prominent tool for estate management, is an establishment in which an arrangement is created by a settlor or grantor to transfer assets to a trustee. The trust, which is managed by a trustee set up by a grantor/settlor, holds property or assets for a specific person or group, called the beneficiary, with the possibility of a settlor of the trust also being one of the beneficiaries.

The terms of the trust relationship and the principles used by the trustee to manage the assets and the distributions to beneficiaries, are outlined in the trust document.

Trusts can be categorized as revocable or irrevocable. In the former, the settlor who funds the trust, reserves the right to rescind the trust relationship and regains the title to the trust assets, whereas in the latter, the settlor does not reserve the right to revoke ownership of assets in the trust, though he/she will have asset protection from claims against the settlor.

The trust can be structured to be a fixed trust, where the distributions to the beneficiaries occur at particular times and in certain amounts as prescribed in the trust document, or discretionary trust, in which the trustee is allowed to determine whether and how much to distribute, basing on the wishes made by the settlor.

Based on the settlor's wishes, a trust can be set up in one of the categories and structures mentioned above to achieve their intended desires. When estate planning is embraced, which encompasses trust establishment, the benefits are enormous but major ones include:

1. Smooth transfer of assets

Assets are transferred after the principal's demise i.e. bequest to the beneficiaries, and in the process, this helps to avoid conflicts among the beneficiaries. Basing on how the trust is categorized and structured, say irrevocable or fixed, the deceased's wishes are fulfilled. Put differently, in the legal fraternity dialect, the deceased's peace will not be disturbed nor are the beneficiaries left mourning but comfortable and secured.

Reference can be made to the recent St. Peter's church demolition in Ndeeba, which is still fresh in our mind. The owner of the land (estate), the late Evelyn Nachwa, a Buganda Kingdom princess willfully gave land to the church but after her demise, the status changed. The estate administrators questioned the donation and, in the process, moved to repossess the land through court. The climax was the demolition of the church after a court order was issued!

2. Assets are protected from creditors and lawsuits

If the trust is structured in such a way that its irrevocable and non–discretionary, no legal claims can be attached to the property of the deceased. This therefore, gives the beneficiaries a peace of mind since at no time can such a claim like "the deceased had uncleared debt to settle" be made against their inheritance.

3. Privacy and confidentiality

Estate planning helps to avoid family secrets relating to the deceased or the incapacitated from getting to the public domain. The details of the distribution and to whom the properties are given, remains confided in the trustee and the beneficiaries.

4. Time and cost–saving

With proper estate planning, cost and time are saved that would be spent in the probate process by stating exactly how, and when the intended beneficiaries receive their inheritance and assume legal rights of ownership than if a sheer will is written.

In conclusion, it is important to note that for successful estate planning, the services of experts in the matters of finance, legal and tax cannot be ignored. It is true this is done at a cost, but the paybacks are worth the investment.

MBARARA CITY HOUSE

www.nssfug.org /nssfug nssfug 0800286773 TOLL FREE

SPACE FOR RENT

Plot 6B, Galt Road

Office Space | Retail Space | Banking Hall | Restaurant | Spacious Parking

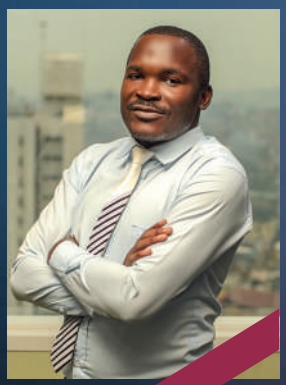
THE PERFECT LOCATION FOR YOUR BUSINESS IS NOW OPEN

Increase your business' success rate today, by renting space at Mbarara's newest and most prime business location.

Mbarara City House has four floors, lifts, ample parking space, 24 hour security, a standby generator and CCTV surveillance systems.

For bookings call: 0752 755 272 | 0782 956 545 | 0755 500 533
or email: realestate@nssfug.org

NSSF a better life



Data Protection, The New Fever.

Is your organization ready?

JOSHUA KIBIRIGE
Anti–Money Laundering Manager,
National Social Security Fund
MBA,BCOM, CPA, CERM, PODITRA, ISO 31000

In 2019, many companies and top executives were still raving about the threats of cyber risk when the Data protection Act was passed to add more regulatory requirements for organizations. Companies now need not to only protect their own assets and intellectual property but also the data collected from customers and other stakeholders.

The Data Protection and privacy Act 2019 imposes onerous responsibility on the data collector, processor and controller. Such responsibilities include but not limited to:

- Informing the data subject of the nature, purpose, category and the period for which the data is being collected.
- Ensuring that the data collected is accurate and up to date
- Protection of data to ensure integrity and confidentiality
- Obtaining the consent of the data subject and obtaining assurance from the host country on whether the host country has adequate data protection measures as envisaged by the Data protection & privacy Act 2019, before his/her personal data is stored and/or processed outside Uganda.
- To allow the data subjects exercise their rights as enshrined in the law e.g.
    - The right to access personal information any time
    - The right to prevent processing of personal data
    - The right to correct or delete personal data

Unfortunately, the enactment of the Data protection & privacy Act 2019 seems to have created opportunities for cyber criminals. Once they get hold of sensitive data, they demand a ransom, which may be millions of dollars, depending on the size of the organization.

For fear of litigation cost and reputation damage, the affected organization may decide to negotiate with the criminal and pay a ransom. Companies such as Carlson Wagonlit Travel (CWT) and Florida City had to part with USD 4.5 million and USD 460,000 respectively, in ransom.

In June 2020, Uganda witnessed the first effects of non–compliance to the regulation when the High court of Uganda awarded a Yunus Lubega Butananziba the plaintiff, damages of 10,000,000 Uganda Shillings for breach of his right to privacy caused by MTN Uganda.

Many organizations have been affected by breaches of data privacy, for example in March 2020, a hotel chain, Marriot, disclosed a data security breach, which affected data of more than 5.2 million hotel guests. According to the Bethesda, Md.–based hospitality giant, the source of the breach was a vulnerability within the application that its hotels use to provide guests with various services. Marriott did not name the specific App.

The Marriot case is just one of the many organizations that have been affected by data breach, including British Airways –USD 230 million, Google Inc–USD 56 million) etc, that have been fined heavily for breach of data privacy regulations during the year 2020 according to the data breach investigation report by Verizon .

Many executives and CEOs are unaware of the momentous amounts of unprotected customer, employee and supplier data that they maintain. For example, confidential information such as staff salaries may be held in a test system, which can be easily accessed by the unauthorized personnel.

As mentioned above, the Act requires any organization that collects, processes and controls customer data to protect the privacy of data subjects by regulating the collection, processing and storage of such data, and providing for the rights of persons from whom data is collected, and guiding the disclosure of personal data.

Risk managers and top executives should be asking the following questions in order to prevent the risk of data breach;

What is the compliance status of our company?

Executives need to be aware of the compliance status of their organizations in order to avoid unnecessary fines and penalties that may result from data breaches.

Where an organization carries out business across borders, even if digitally, it should ensure that it meets the data compliance requirements for all the sensitive data collected. For instance, if data is processed and stored outside Uganda, the data controller is required to establish whether there are adequate controls for data protection in the host country as stipulated in the data protection and privacy Act 2019.

Is data protected even when devices are not connected on the organization network?

Following the new normal of working from home, many employees now take sensitive information away from the work place. Remote working entails increased mobility of devices, i.e, laptops and mobile phones, which can easily be stolen or misplaced, hence increasing the risk of data breach.

It is important that managers employ data protection strategies that work, both on–site and off–site.

Does the culture in the organization support data protection?

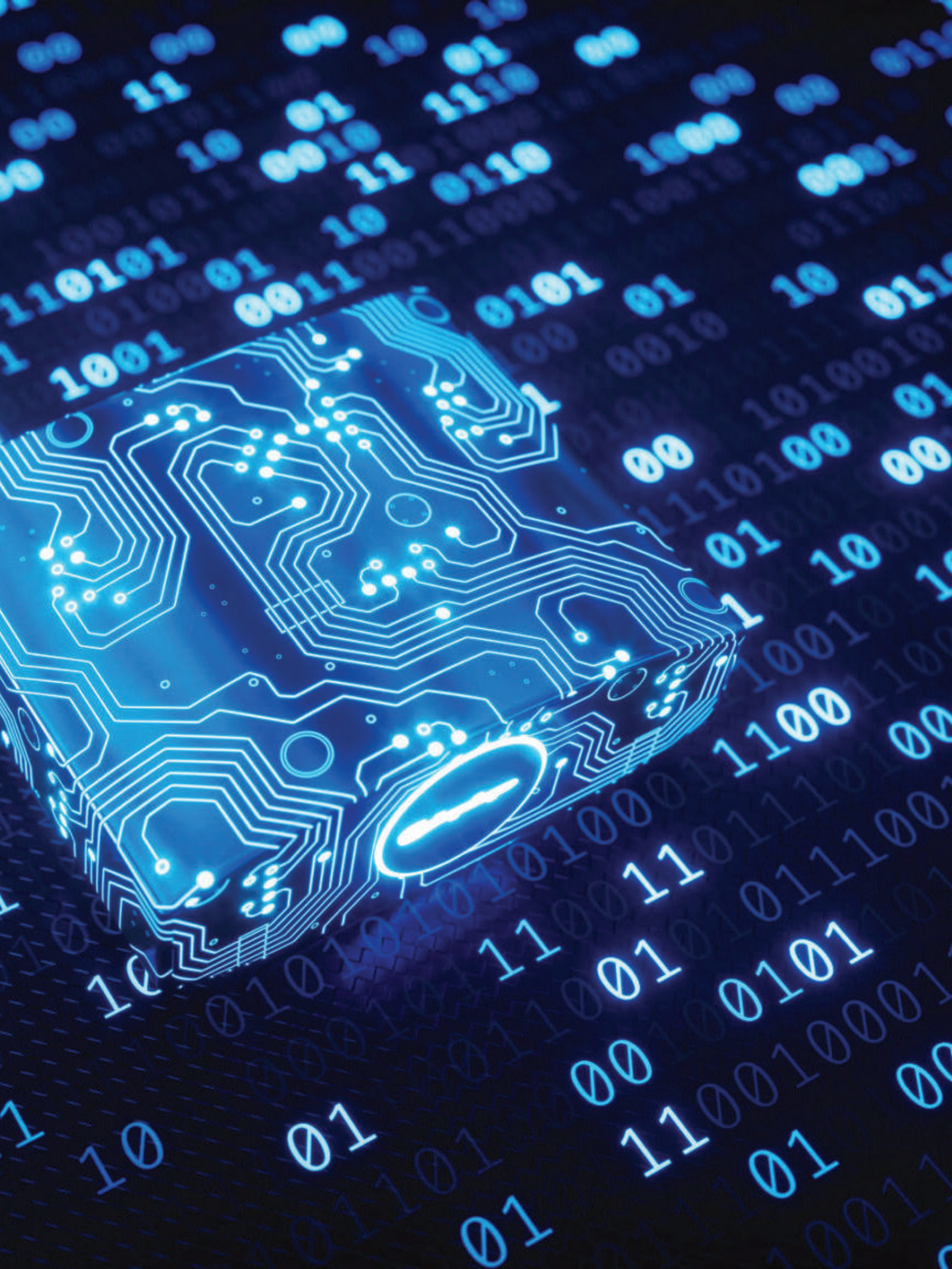
While organizations are required to have a data protection officer, it should be every employee's responsibility to have an understanding of the requirements of the Data protection and privacy Act, 2019, and ensure compliance of the same; with everyone taking accountability for how the company collects, uses and shares personal information for the customers or suppliers.

The data flow in the organization should be mapped to ensure there is visibility on how data is being managed.

Data protection culture should be demonstrated in the way in which the customer service staff talk to company customers about data privacy, by being open in how their data is used and protected. The end user should have a transparent view and a say in the processing of his/her personal data.

Conclusion

As I conclude, it is important to note that with the Data Protection Act, 2019 in place, cybercriminals, now know the value attached to personal data, and any organization that neglects its responsibility of data protection will suffer severe consequences.



JESSE OKUTRE
Investment Risk Analyst,
National Social Security Fund
MBA, BECON, CERM, CRA.

Cyber abuse:
Are your children safe?

With many countries gradually lifting restrictions on the lockdown, schools are one of the areas that generally remain locked. Consequently, a number of schools have turned to online classes as a way of ensuring continuity of learning, despite continued school closure. It means children are spending more time online or using the internet to attend classes and communicate with friends, than ever before.

I recently witnessed my neighbor very angry and ferociously beating her 12–year–old daughter, while showing her pictures and videos on a phone. I intervened and stopped the beating because I was concerned that the girl was in danger of being severely injured. I noticed that my neighbor was reacting to the explicit videos and pictures the daughter had recorded and tried to send to a friend she met online.

As the COVID–19 virus continues to spread in the country, it is unlikely that schools will be allowed to fully operate. So online classes and working from home are bound to continue, as people adhere to the measures against the spread of coronavirus. This gives children a lot of time and exposure to the internet.

During this time, there has been a rise in TV watch time, online gaming, and social media is awash with videos and pictures, e.g. TikTok, Snapchat, etc. According to The International Watch Foundation, at the start of the lockdown, internet users reported more images and videos (44,809) than in 2019 (29,698), all uploaded by children. With data and time availability, children will be curious and explore websites other than just attending online classes.

If the parents do not supervise internet usage, children could be exposed to cyber abuse, which includes but is not limited to the following:

1) Exposure to pedophilias and rapists

People make hundreds of friends on social media, and may not know the intentions of some of the people they meet online. Pedophiles usually target children online, through school websites. By promising to be best friends and convincing them to keep everything as a secret, a child can easily be a victim of rape by an unknown person, met online.

2) Explicit content and soft porn

Many influencers on social media upload content that may not be good for children; such content can significantly influence bad child behavior in form of outfits worn, ways of talking, and lifestyle.

3) Early relationships and kidnappers

Online child relationships are common these days. Online predators scan through the website (could be online games, classes, etc.), to find easy prey. The predator will engage the child in conversations, pretending to be his/her classmate or neighbor, and naively, the child will assume the predator is an innocent friend, while the predator is laying a trap to kidnap the child

4) Cyberbullying

Cyberbullying can be impersonation, uploading inappropriate pictures of the child, harassment by texting, or video shaming. This can have severe repercussions on children, if not addressed. Some children develop an inferiority complex, and some even commit suicide. There are many other forms of abuse on the internet that children could be exposed to.

However, not all is lost, there are certain control measures that could help mitigate the risks.

a) Monitoring your children's activities online

Parents can reduce the risk of exposure to predators by monitoring their children's online friends and the people they spend time chatting with, and generally viewing the children's content on the websites.

It is easy to assume that a child in front of a PC is attending online classes, yet the child may be watching a video. Continually checking on the kids attending online classes could help curb some of the predators attempting to befriend children online.

b) Use of technological measures

i) Smartphones and computers have applications that can record the activities they execute, giving details of the time spent and websites accessed. The reports generated by the apps can help parents analyze the child's actions on the internet.

ii) Installing applications that block unwanted content can go a long way in protecting children from cyber abuse. For example, security apps can help block unwanted content.

iii) Creating screen limits and phone curfews to prevent children from engaging in late–night chats with strangers online or internet friends can help deter predators from pretending to be "secret friends" on the internet.

c) One–on–one with your child

Parents can innocently ask the children what they have learned on a particular day. This could help give a hint or clue, as to what the child is up to.

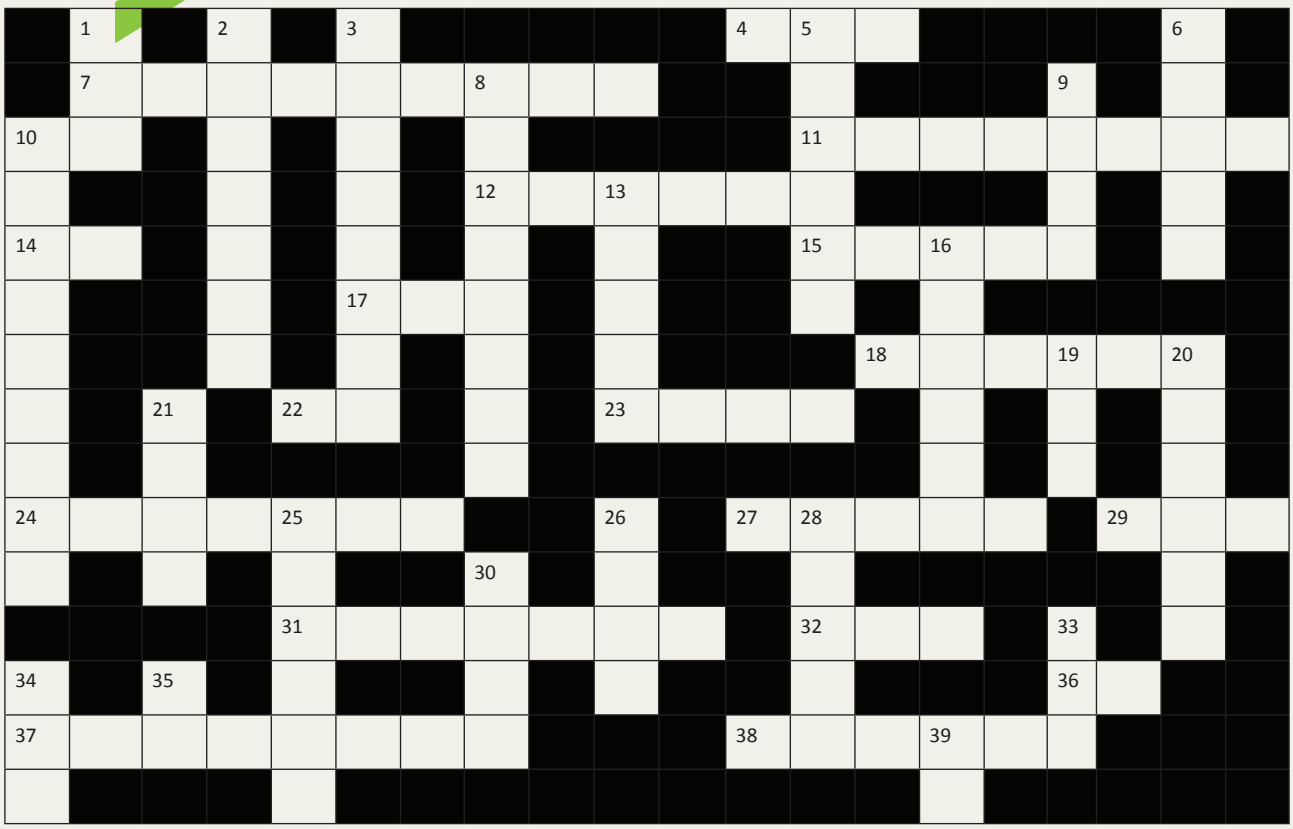
Conclusion

The number of children using the internet is on the rise; this will continue even after coronavirus restrictions are lifted. Putting safeguards in place to ensure safe and appropriate use of the internet by children, cannot be overemphasized. The internet, whether on a computer or a mobile phone, has or is increasingly becoming a way of life. It is not beneficial to completely bar children from using the internet, because it enhances learning and exposes the children to a number good things. But this has to be done in a secure environment, and you as a parent have the biggest role to play in ensuring a secure environment for your children.

Risk Knowledge Crossword Puzzle

ISSUE No.2

ROBERT MASIGA
Operational Risk Officer,
National Social Security Fund
BSTAT, CFA Level III



ACROSS

4. A device, or software application that monitors a network or systems for malicious activity or policy violations, abbr.3

7. Risk resulting into an individual outliving planned retirement income,9

11. Risk mitigation technique that involves shifting risk to a third party,8

12. All the money and property owned by a person, especially at death,6

14. A type of investment security that typically pays investors fixed return until its maturity, abbr.2

15. Denotes a relationship with information technology,5

17. A phase of the software testing at the tail end of the process, abbr.3

18. Making no effort to reduce or mitigate risk and consider it bearable,6

22. A type of AI that allows software applications to become more accurate at predicting outcomes, abbr.2

23. Tools and machines that may be used to solve real–world problems, short form,4

24. One form of phishing, 7

27. Versatile seagoing vessels, 5

29. Color for denoting risk rating where likelihood and impact are high,3

31. A legal process to determine the authenticity of a will,7

32. A collection of systems used to protect the copyrights of electronic media. Abbr,3

36. Pension scheme where the amount paid is based on number of years worked and the salary earned, abbr.2

37. An individual or organisation that attempt to destroy, expose, alter, disable, steal or gain unauthorized access to an electronic asset,8

38. Another word for “infrequent”,6

DOWN

1. A set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users, abbr.3

2. An insurance contract that promises to pay a fixed regular income,7

3. Amount of risk that remains after controls are applied,8

5. Third function in Cyber Defense Matrix used after an event, 6

6. Color used to denote risk rating where likelihood and impact are very low,5

8. First function in Cyber Defense Matrix used prior to an event,8

9. A person who operates something,4

10. If a control is adequate in substantially reducing the risk, it is said to be,9

13. An establishment that manages an individual's estate after demise,5

16. A file or other item of data made in case the original is lost or damaged,6

19. Is an electronic exchange of money, abbr.3

20. A person or thing likely to cause damage or danger, 6

21. A white box method of testing information security system, abbr,4

25. Can also mean a marked effect or consequence of risk,6

26. Things known or assumed as facts, making the basis of reasoning.4

28. An investment made with the intention of reducing the risk of adverse price movements in an asset,5

30. Provides an annual analysis of security incidents and data breaches, abbr.4

33. Cyber Defense Matrix, abbr.3

34. Blocks malicious attempts to web applications, abbr.3

35. Use of computers to process data.abbr.2

39. Pension scheme where own and employer's contributions are both invested, and the proceeds paid to the beneficiary as a lump–sum.abbr.2

SOLUTION TO ISSUE No.1