

IT Risk Management Practices in Kenya

Stanley Chege¹, Gregory Wanyembi², Constantine Nyamboga³
Enterprise Computing, Computing and Informatics, Mount Kenya University, Thika, Kenya.

Abstract: Risk management is the process of identifying, assessing and controlling threats to an organization's capital and earnings. These threats, or risks, could stem from a wide variety of sources, including financial uncertainty, legal liabilities, strategic management errors, accidents and natural disasters. IT security threats and data-related risks, and the risk management strategies to alleviate them, have become a top priority for digitized companies. As a result, a risk management plan increasingly includes companies' processes for identifying and controlling threats to its digital assets, including proprietary corporate data, a customer's personally identifiable information (PII) and intellectual property.

Keywords: Risk, Threat, Vulnerability, Assets, Business Continuity Management, Risk Assessment, Risk Appetite, ISO 31000. Cyber Security.

I. Problem Statement

Some managers have been prosecuted for causing organization failures occasioned by inadequate risk management and internal controls (Financial Times, 2019). From the onset of Sarbanes-Oxley Act (SOX) of 2002 to the Dodd-Frank Act of 2010, more managers have embarked on the compliance journey to the risk management and corporate governance regulations. These regulations help to restore investor confidence. The legislations created regulatory processes to limit risk by enforcing transparency and accountability. Risk management is part of business strategy and priority for leading organizations. The general business problem is that managers lack strategies to drive risk management. The specific business problem is that some managers in Kenya lack strategies to manage the strategic operational, financial, market, credit, legal and reputation risks.

II. Literature Review

Risk management is the continuing process to identify, analyze, evaluate, and treat loss exposures and monitor risk control and financial resources to mitigate the adverse effects of loss (Marquette, 2019).

As the outcomes of business activities are uncertain, they are said to have some element of risk. These risks include strategic failures, operational failures, financial failures, market disruptions, environmental disasters, and regulatory violations. Risk is a statistical concept that is measured using statistical concepts that are related to the unknown future. Almost all investments are exposed to it. Risk management involves identifying the types of risk exposure within the company, measuring those potential risks, proposing means to hedge, insure or mitigate some of the risks and estimating the impact of various risks on the future earnings of the company (CioIndex, 2019). While it is impossible that companies remove all risk from the organization, it is important that they properly understand and manage the risks that they are willing to accept in the context of the overall corporate strategy. The management of the company is primarily responsible for risk management, but the board of directors, internal auditor, external auditor, and general counsel also play critical roles. Risk can be managed in several ways: by the buying of insurance, by using derivative instruments as hedges, by sharing risks with others, or by avoiding risky positions altogether (Financial Times, 2019).

III. Why Risk Management

Risk management's objective is to assure uncertainty does not deflect the endeavor from the business goals. Risks can come from various sources including uncertainty in financial markets, threats from project

failures (at any phase in design, development, production, or sustainment life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters, deliberate attack from an adversary, or events of uncertain or unpredictable root-cause. There are two types of events i.e. negative events can be classified as risks while positive events are classified as opportunities.

IV. 10 Steps to Cyber Security

The 10 steps to cyber security was originally published in 2012 and is now used by a majority of the FTSE350. They are set up the Risk Management Regime. Network Security. User education and awareness. Malware prevention. Removable media controls. Secure configuration and patches. Managing user privileges. Incident management. Monitoring. Home and mobile working.

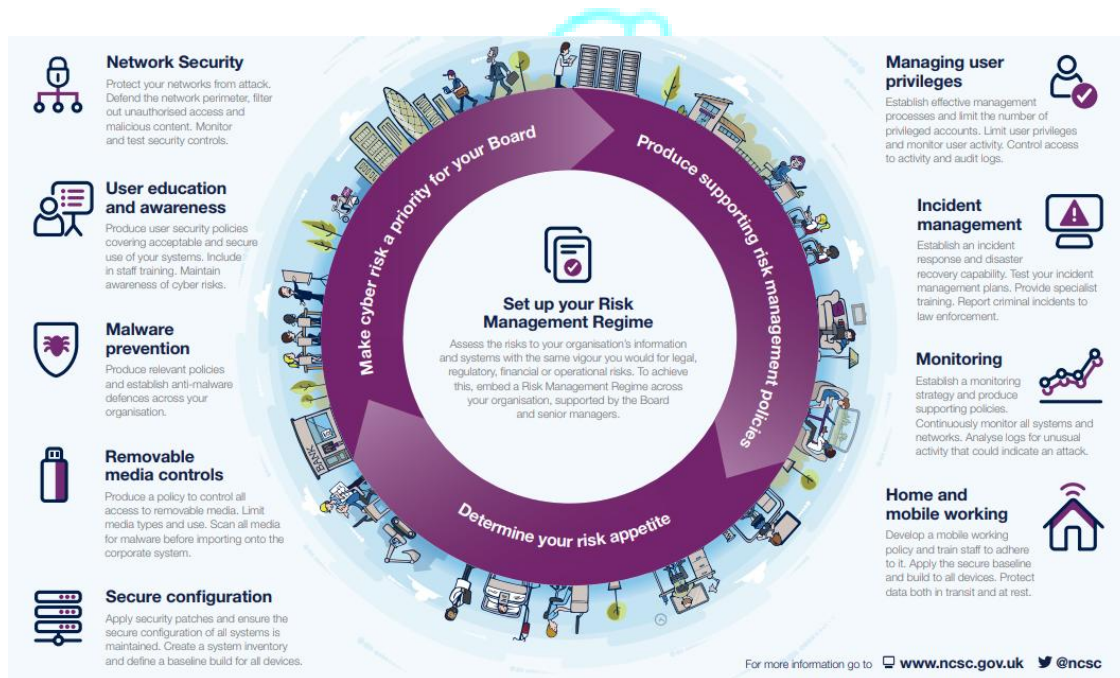


Figure 1. 10 Steps to Cyber Security. Source: (NCSC, 2019).

V. Risk Management Example

Proper risk management implies control of possible future events and is proactive rather than reactive. For example: An activity in a network requires that a new technology be developed. The schedule indicates six months for this activity, but the technical employees think that nine months is closer to the truth. If the project manager is proactive, the project team will develop a contingency plan. When the 3 weeks deadline approached, and it appeared that the project would not be completed, crisis management became the mode of operation (BIA, 2019).

VI. Risk Management Standards

Several standards have been developed worldwide to help organizations implement risk management systematically and effectively. These standards seek to establish a common view on frameworks, processes and practice, and are generally set by recognized international standards bodies or by industry groups. Risk management is a fast-moving discipline and standards are regularly supplemented and updated. The different standards reflect the different motivations and technical focus of their developers and are appropriate for

different organizations and situations. Standards are normally voluntary, although adherence to a standard may be required by regulators or by contract (TheIRM, 2019).

Commonly used standards include:

- ISO 31000 2009 – Risk Management Principles and Guidelines
- A Risk Management Standard – IRM/Alarm/AIRMIC 2002 – developed in 2002 by the UK’s 3 main risk organizations.
- ISO/IEC 31010:2009 – Risk Management - Risk Assessment Techniques
- COSO 2004 – Enterprise Risk Management - Integrated Framework
- OCEG “Red Book” 2.0: 2009 – a Governance, Risk and Compliance Capability Model

VII. Risk Management Factors

Factors to Consider in Risk Management

There are some specific factors to consider when examining project, product, and business risks. Some examples of these factors are listed here, although this list is meant to stimulate your thinking rather than to be an all-inclusive list (NCSU, 2019).

- People risks are associated with the availability, skill level, and retention of the people on the development team.
- Size risks are associated with the magnitude of the product and the product team. Larger products are generally more complex with more interactions. Larger teams are harder to coordinate.
- Process risks are related to whether the team uses a defined, appropriate software development process and to whether the team members follow the process.
- Technology risks are derived from the software or hardware technologies that are being used as part of the system being developed. Using new or emerging or complex technology increases the overall risk.
- Tools risks, like technology risks, relate to the use, availability, and reliability of support software used by the development team, such as development environments and other Computer-Aided Software Engineering (CASE) tools.
- Organizational and managerial risks are derived from the environment where the software is being developed. Some examples are the financial stability of the company and threats of company reorganization and the potential of the resultant loss of support by management due to a change in focus or a change in people.
- Customer risks are derived from changes to the customer requirements, customers’ lack of understanding of the impact of these changes, the process of managing these requirements changes, and the ability of the customer to communicate effectively with the team and to accurately convey the attributes of the desired product.
- Estimation risks are derived from inaccuracies in estimating the resources and the time required to build the product properly.
- Sales and support risks involve the chances that the team builds a product that the sales force does not understand how to sell or that is difficult to correct, adapt, or enhance.

Spontaneous and sporadic risk identification is usually not sufficient. There are various risk elicitation techniques the team can use to systematically and proactively surface risks:

- Meeting. The team, including the development team and the marketing and customer representatives if possible, gathers together. The group brainstorms; each participant spontaneously contributes as many risks as they can possibly think of.
- Checklists/Taxonomy. The risk elicitors are aided in their risk identification by the use of checklists and/or taxonomies (in other words, a defined, orderly classification of potential risks) that focuses on some subset of known and predictable risks. Checklists and taxonomies based upon past projects are especially beneficial. These artifacts should be used to interview project participants, such as the client, the developers, and the manager.
- Comparison with past projects. The risk elicitors examine the risk management artifacts of previous projects. They consider whether these same risks are present in the new project.
- Decomposition. Large, unwieldy, unmanageable risks that are identified are further broken down into small risks that are more likely to be managed. Additionally, by decomposing the development process into small pieces, you may be able to identify other potential problems.

VIII. Types of Risks

IT risk can involve a range of threats, from the everyday to the unthinkable, with varying levels of likelihood and impact. These threats can be grouped into three categories: Data-driven risks, business-driven risks and event-driven risks (IBM, 2019).

- Data-driven risks: From an IT perspective, data-driven risks often receive the most attention. Generally, they occur more frequently than other types of risks, but the financial loss from any one occurrence is relatively low. These risks have some crossover with business-driven risk in terms of business continuity and business availability, but their focus is at the system or data level.
- Business-driven risks: Business-driven risks directly impact business continuity and business operations. An organization's board members would typically be most concerned about these risks because they are generally more strategic in nature than data-driven risks and have business wide ramifications.
- Event-driven risks: Any event that disrupts an organization's workforce, processes, applications, data or infrastructure can be classified as an event-driven risk. These risks affect business continuity and viability.

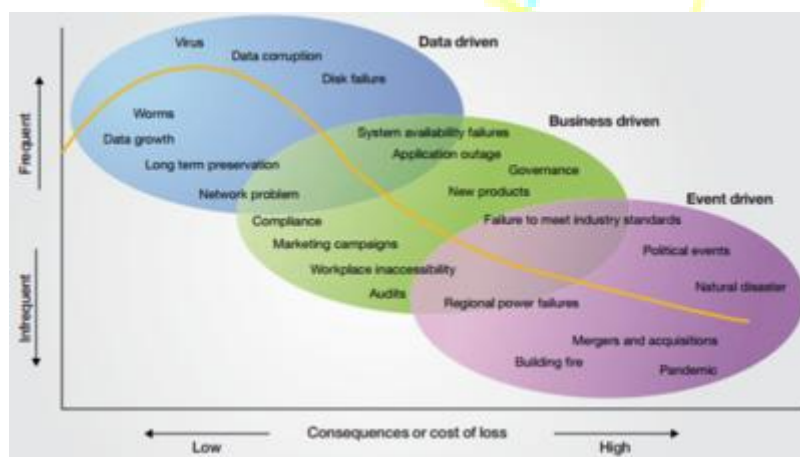


Figure 2. Source: (IBM, 2019).

How to Manage Risk in the Enterprise?

IX. Effectively Managing IT Risk requires

- Evaluating how a disruption or corruption of IT services could threaten and impact critical business services
- Effectively identifying and measuring IT risk to the business
- Defining strategies for managing those risks judiciously
- Defining and implementing an ongoing IT risk management and governance program
- Monitoring IT risks on a continuous basis and taking appropriate, timely actions to mitigate the risk to business services

Risk Management Requirements

X. Requirements for Getting Risk Management Started

- Senior leadership commitment and participation is required.
- Stakeholder commitment and participation is required.
- Risk management is made a program-wide priority and "enforced" as such throughout the program's life-cycle.
- Technical and program management disciplines are represented and engaged. Both program management and engineering specialties need to be communicating risk information and progress toward mitigation. Program management needs to identify contracting, funding concerns, SEs need to engage across the team and identify risks, costs, and potential ramifications, if the risk were to occur, as well as mitigation plans (actions to reduce the risk, and cost/resources needed to execute successfully).
- Risk management integrated into the program's business processes and systems engineering plans. Examples include risk status included in management meetings and/or program reviews, risk mitigation plan actions tracked in schedules, and cost estimates reflective of risk exposure (Mitre, 2019)

XI. Risk Management Strategy

These are the 5 risk management strategies that you can use to manage risk on your project. You'll probably find yourself using a combination of techniques, choosing the strategies that best suit the risks on your project and the skills of your team. However, you decide to approach risk, make sure that you log the action plan in your risk log and keep it up to date with the latest progress towards managing your risks.

1. Accept the Risk: Accepting the risk means that while you have identified it and logged it in your risk management software, you take no action. You simply accept that it might happen and decide to deal with it if it does. This is a good strategy to use for very small risks – risks that won't have much of an impact on your project if they happen and could be easily dealt with if or when they arise. It could take a lot of time to put together an alternative risk management strategy or take action to deal with the risk, so it's often a better use of your resources to do nothing for small risks.

2. Avoid the Risk: You can also change your plans completely to avoid the risk. This is a good strategy for when a risk has a potentially large impact on your project. For example, if January is when your company Finance team is busy doing the corporate accounts, putting them all through a training course in January to learn a new process isn't going to be a great idea. There's a risk that the accounts wouldn't get done. It's more likely, though, that there's a big risk to their ability to use the new process, since they will all be too busy in January to attend the training or to take it in even if they do go along to the workshops. Instead, it would be better to avoid January for training completely. Change the project plan and schedule the training for February when the bulk of the accounting work is over.

3. Transfer the Risk: Transference is a risk management strategy that isn't used very often and tends to be more common in projects where there are several parties. Essentially, you transfer the impact and management of the risk to someone else. For example, if you have a third party contracted to write your software code, you could transfer the risk that there will be errors in the code over to them. They will then be responsible for managing this risk, perhaps through additional training. Normally transference arrangements are written up into project contracts. Insurance is another good example. If you are transporting equipment as part of your project and the van is in an accident, the insurance company will be liable for providing new equipment to replace any that was damaged. The project team acknowledges that the accident might happen, but they won't be responsible for dealing with sourcing replacement kit, moving it to the right location or paying for it as that is now the responsibility of the insurance company.

4. Mitigate the Risk: Mitigating against a risk is probably the most commonly mitigation of risk used risk management technique. It's also the easiest to understand and the easiest to implement. What mitigation means is that you limit the impact of a risk, so that if it does occur, the problem it creates is smaller and easier to fix. For example, if you are launching a new washing machine and the Sales team then have to demonstrate it to customers, there is a risk that the Sales team don't understand the product and can't give good demonstrations. As a result, they will make fewer sales and there will be less revenue for the company. A mitigation strategy for this situation would be to provide good training to the Sales team. There could still be a chance that some team members don't understand the product, or they miss the training session, or they just aren't experts in washing machines and never will be, but the impact of the risk will be far reduced as most of the team will be able to demonstrate the new machine effectively. You can mitigate against the impact, like in this example, and you can also mitigate against the likelihood of it happening. Sometimes the actions will be broadly the same; sometimes you'll have to have some tasks to reduce the chance that the risk happens and some separate tasks to make the impact of the risk smaller if it happens.

5. Exploit the Risk: Acceptance, avoidance, transference and mitigation are great to use when the risk has a negative impact on the project. But what if the risk has a positive impact? For example, the risk that the new washing machines are so popular that we don't have enough Sales staff to do the demonstrations? That's a positive risk – something that would have a benefit to the project and the company if it happened. In those cases, we want to maximize the chance that the risk happens, not stop it from happening or transfer the benefit to someone else!

Exploitation is the risk management strategy to use in these situations. Look for ways to make the risk happen or for ways to increase the impact if it does. We could train a few junior Sales admin people to also give washing machine demonstrations and do lots of extra marketing, so that the chance that there is lots of interest in the new machine is increased, and there are people to do the demos if needed (DBP Management, 2019).

XII. Risk Management Cycle

The illustration below provides an example Risk Management Cycle that can be adopted and implemented by an institution after identifying and characterizing risks and determining its appropriate risk mitigation strategies.

- **Define Commitment to Risk Management:** This is where the institution establishes its goals or desired outcomes for its risk management program. A goal or outcome, however, cannot be established until risks are identified and characterized. The commitment to risk management example could be a defined commitment for an IACUC to have no protocol related non-compliant items (NCIs) on USDA inspection reports. The commitment to no NCIs represents a Prevention strategy by the institution based on the identification and characterization of what could happen if there are NCIs on any given USDA inspection report. In other words, the institution deems the occurrence of protocol related NCIs on a USDA inspection report to carry such a serious impact that it determines that prevention is the best method for mitigating this risk.
- **Design Risk Management Framework:** Designing a risk management framework means that the institution must be aware of all available actions, procedures, and/or processes, and potentially create

some of their own. For the purposes of our example, an IACUC can look at a variety of methods to ensure that the protocols are well written, cover all aspects of the USDA Animal Welfare regulations, and are followed by compliant PIs. To continue with our example, we will say that the IACUC has chosen two methods for its risk management framework: protocol audits and focused pre-review of protocols describing animal research activities on USDA covered species.

- **Implement Framework:** In this step, the institution must modify its operations to encompass the activities of the framework. Organizations or departments unused to creating new procedures or new programs may struggle with this step. Indeed, many risk programs fail because they are unable to operationalize what they said they wanted to do in order to mitigate risk. Such operationalization may include hiring new individuals, designing new jobs, reassigning work duties, creating new policies and procedures, training, changing documentation or electronic systems, and potentially creating an entirely new organizational culture. This can quickly become daunting and complex. The easiest way to approach this is to start with small changes that give you quick wins. You can build up on those easy and small successes with ever increasingly large changes until you arrive at your framework. Within our example, the audits of on-going protocols would need to be scheduled (after the auditing personnel are identified as well as trained and auditing procedures are codified) and pre-review initiated (again, after the same steps as to implement auditing).
- **Monitor Outcomes:** Prior to initiating any changes and new activities, a reasonable timeframe for benchmarking success should be established. That timeframe allows for the new framework to be initiated, fully implemented, and undergo preliminary evaluation (in our example, this would be a USDA inspection). Outcomes (e.g. the USDA inspection report and additional feedback received at the time of the inspection) should then be thoroughly reviewed.
- **Improve Processes:** Based on the review of the outcomes, modifications can be made to further improve outcomes and/or address shortcomings. To finish my example, this would be the time to review the USDA inspection report, assess the findings including if NCIs were included in the report, and determine if any changes need to be made to prevent the appearance of NCIs on future USDA inspection reports based on the reported NCIs and feedback ((Laboratory Equipment, 2019).



Figure 3. Source: (Laboratory Equipment, 2019).

What is important to remember about this Risk Management Cycle is that at any time the laws, regulations, guidelines, or other guidelines may change. At that time, you must re-enter the cycle by defining what your new commitment to risk management is based on the change. Commitments and strategies most certainly change when regulations and guidelines change, and institutions should not be too concerned about making a change. Making changes in accordance with regulatory changes can not only keep institutions up-to-date with current regulatory expectations but can also help to decrease self-imposed regulatory burden.

XIII. 10 Key Ideas for Risk Management







	Be proactive about managing risk or you'll constantly be in crisis-driven, fire-fighting mode.
	Systematically surface risks by meeting with marketing and the customer, by using checklists and taxonomies, by comparing with past projects, and by decomposing large, unwieldy risks into smaller, more manageable risks.
	All the stakeholders must communicate about risks throughout the entire development cycle. Communication is at the center of the risk management process.
	Prioritize risks by computing the risk exposure of each risk. Sort the list of risks based upon the risk exposure and proactively manage those on the top of the list.
	Develop a "Top 10" risk list for your projects. It is likely that this "Top 10" list will contain risks that will appear on your next projects as well.
	Utilize a risk-driven process for choosing between an agile and a plan-driven process, or a hybrid of the two.

Figure 4. source: (North Carolina State University, 2019)

In the risk management cycle, product and project risks are identified, analyzed, and prioritized. The top-ranking risks are planned and mitigated. All risks are monitored. It is important for a project to focus on its critical success factors while keeping an eye on its risk factors. Risk management practices enable the team to find the opportunity in the risk items. Be proactive (North Carolina State University, 2019).

XIV. Principles of Risk Management

There are specific core principles regarding risk management. When looking to perform an actual risk assessment, the following target areas should be part of the overall risk management procedure (as defined by the International Standards Organization; ISO):

- The process should create value
- It should be an integral part of the organizational process
- It should factor into the overall decision-making process
- It must explicitly address uncertainty
- It should be systematic and structured
- It should be based on the best available information
- It should be tailored to the project
- It must consider human factors
- It should be transparent and all-inclusive
- It should be dynamic and adaptable to change
- It should be continuously monitored and improved upon as the project moves forward (Programsuccess, 2019.)

Risk Management Implementation Process

XV. Risk Management Process

The following diagram illustrates the six steps of the risk management process: identify, analyze and prioritize, plan and schedule, track and report, control, and learn. It is important to understand that the process of managing each risk goes through all of these steps at least once and often cycles through numerous times. Also, each risk has its own timeline, so multiple risks might be in each step at any point in time.

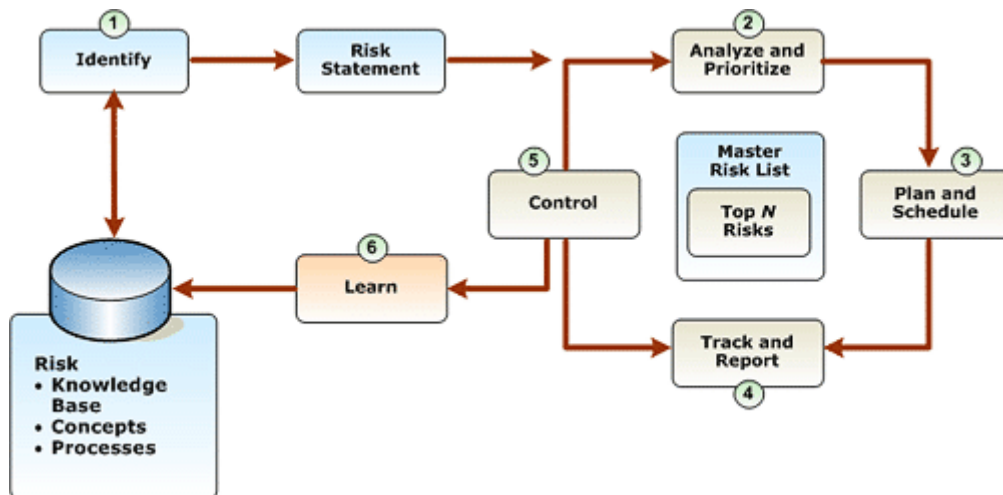


Figure 5. Source: (Microsoft, 2019).

- Identify - Risk identification allows individuals to identify risks so that the operations staff becomes aware of potential problems. Not only should risk identification be undertaken as early as possible, but it also should be repeated frequently.
- Analyze and prioritize - Risk analysis transforms the estimates or data about specific risks that developed during risk identification into a consistent form that can be used to make decisions around prioritization. Risk prioritization enables operations to commit resources to manage the most important risks.
- Plan and schedule - Risk planning takes the information obtained from risk analysis and uses it to formulate strategies, plans, change requests, and actions. Risk scheduling ensures that these plans are approved and then incorporated into the standard day-to-day processes and infrastructure.
- Track and report - Risk tracking monitors the status of specific risks and the progress in their respective action plans. Risk tracking also includes monitoring the probability, impact, exposure, and other measures of risk for changes that could alter priority or risk plans and ultimately the availability of the service. Risk reporting ensures that the operations staff, service manager, and other stakeholders are aware of the status of top risks and the plans to manage them.
- Control - Risk control is the process of executing risk action plans and their associated status reporting. Risk control also includes initiating change control requests when changes in risk status or risk plans could affect the availability of the service or service level agreement (SLA).
- Learn - Risk learning formalizes the lessons learned and uses tools to capture, categorize, and index that knowledge in a reusable form that can be shared with others.

Risk Management Framework

XVI. The Risk Management Framework (See Figure 5.)

Risk Management is the art and science of thinking about what could go wrong, and what should be done to mitigate those risks in a cost-effective manner. To identify risks and figure out how best to mitigate

them, a framework is needed for classifying risks. All risks have two dimensions to them: likelihood of occurrence, and severity of the potential consequences. These two dimensions form four quadrants, which in turn suggest how we might attempt to mitigate those risks (CayenneConsulting, 2019).

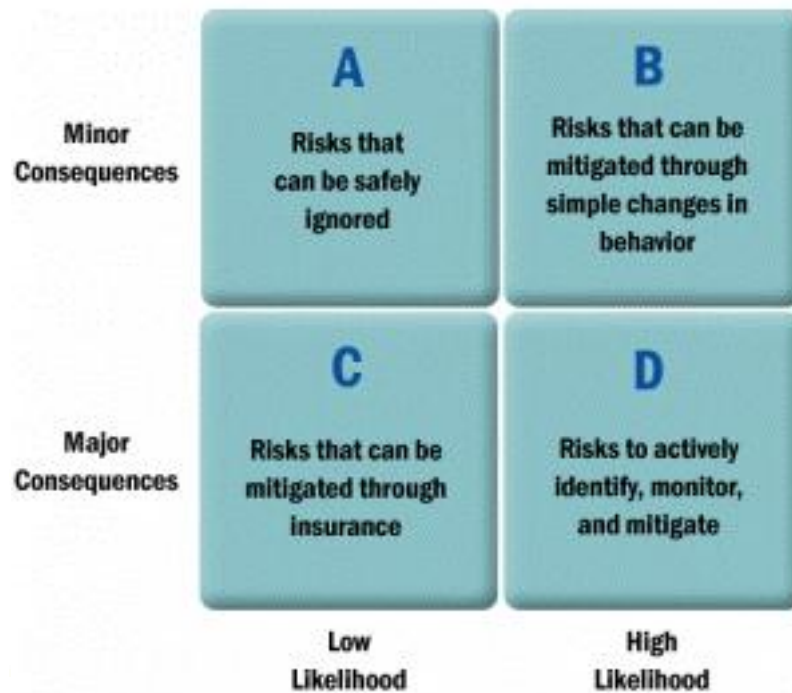


Figure 6. Source: (CayenneConsulting, 2019).

Once we know the severity and likelihood of a given risk, we can answer the question: Does the benefit of mitigating a risk outweigh the cost of doing so?

- Quadrant A: Ignorable Risks: Cost effectiveness is an important consideration in deciding how we face up to risks. Risks with relatively minor consequences and a relatively low likelihood of occurring – those in Quadrant A of our framework – obviously aren't worth spending a lot of time worrying about. An example of a low-likelihood, minor-consequence risk might be the possibility of getting a flat tire on your way to a routine meeting. Assuming you service your car regularly and you drive on maintained roads, a flat tire might cause you to be late to a meeting once every ten years. It's not a big deal.
- Quadrant B: Nuisance Risks: The next category of risks are those we call "nuisance risks" – little things that often seem to go wrong, but whose impacts are easy enough to minimize through straightforward changes in behavior. There are countless examples of nuisance risks and simple solutions:
 - The printer runs out of toner while you're preparing the proposal for the customer meeting that starts in 30 minutes. Solutions: don't wait until the last minute, and always keep extra toner on hand.
 - Your lead engineer gets the flu three days before the scheduled release date of your first customer beta. Solutions: create a development process free of dependencies on any one person and build in contingencies for the fact that almost everything seems to take twice as long and cost twice as much as you originally expect.
 - You knock a mug of coffee into your laptop keyboard and coat your hard drive in cream and sugar, making your marketing plan inaccessible. Solution: use software to perform automated daily backups so that you'll lose, at most, a day of work if you destroy your computer.

With a little common sense, nuisance risks shouldn't cause any lost sleep.

- **Quadrant C: Insurable Risks:** Risks that could have major consequences but are relatively unlikely to happen are often insurable. Insurance is the practice of spreading the cost of an improbable loss across a group, so that no single individual bears the entire cost of a disaster. Everybody pays a premium to the insurance company, and the insurance company pays claim benefits when one of its customers experiences an insured loss. Here are a few common forms of insurance and the risks they cover:
 - Property & Casualty Insurance can mitigate losses from fire, theft, and natural disasters;
 - Key Executive Insurance can mitigate losses from the death or incapacitation of a management team member;
 - Liability Insurance can mitigate lawsuits resulting from product defects or on-site injuries to visitors;
 - Errors & Omissions Insurance can mitigate lawsuits from disgruntled customers; and
 - Directors & Officers Insurance can mitigate lawsuits in cases of negligence, harassment, or discrimination.

Even uncommon risks are often insurable. Some underwriters specialize in writing unusual policies: event cancellations due to adverse weather; or injury to specific body parts (early examples include Jimmy Durante, who insured his nose for \$50,000, and Fred Astaire, who insured his legs for \$75,000).

- **Quadrant D: The Company Killers:** Now we come to the Company Killers: the risks with both a relatively high likelihood of occurrence and major consequences. These risks can sink startups and Fortune 500 companies alike. The survival of your venture depends on your ability to identify and mitigate the company killers. The thing that makes company killers so deadly is that there are so many of them. Individually, they may seem manageable, but collectively, they represent a true challenge for any entrepreneur. For example, suppose you manage to distill your world down to just ten company killers and you think you've eliminated 90% of the risk in each category:

There's a 90% chance that you've identified a genuine market need;
There's a 90% chance that your addressable market is as big as you think it is;
There's a 90% chance that you can actually implement your innovation;
There's a 90% chance that you can figure out how to sell it for more than it costs you to make it;
There's a 90% chance that you have assembled the right management team to do the job;
There's a 90% chance that you manage to stay one step ahead of the competition;
There's a 90% chance that you don't get sued into bankruptcy;
There's a 90% chance that you won't get buried in regulatory red tape;
There's a 90% chance that you don't run out of money; and
There's a 90% chance that nothing else goes wrong.
You might take comfort in the fact that any one of these risk factors presents only a 10% chance of sinking the company. However, the probability of surviving all ten risk factors (making a technical assumption that the ten risk factors are statistically independent of each other) is:
 $90\% \times 90\% \times 90\% \times 90\% \times 90\% \times 90\% \times 90\% \times 90\% \times 90\% \times 90\% = 35\%$
The key insight here is that a company that is reasonably good at managing individual risks might have a marginal chance of surviving overall. That's why "reasonably good" isn't good enough – risk management must be among the entrepreneur's core competencies.

XVII. Reasons for Failure in Implementing Risk Management

As time passes experience has been gained both nationally and internationally in respect of what functions and what does not function. Some of the elements that have had greatest negative impact are, in our opinion, the following (IIA Norge, 2019):

- Lack of clarity in vision and common values as well as badly formulated strategies and objectives which in turn lead to lack of co-operation and focus in the organization.
- Lack of a link between strategic objectives and risk management.
- Imprecise mandate leading to lack of understanding of the role of the Risk Management function and the division of responsibilities.
- The Head of Risk Management does not possess competency in risk management, strategy and the wider picture so that he/ she is not able to take on the role of advisor and challenger.
- The Head of Risk Management does not understand the business.
- The risk management concepts are not understood or are misunderstood.
- Lack of ownership of the system tool used.
- A tool is used without understanding its weaknesses and limitations.
- Discussion is not encouraged; no effort is made to promote an honest and open evaluation of risk – “nobody should risk having their head cut off for telling it as it is”.
- Lack of prioritization of significant risks.
- Lack of understanding/ knowledge of correlation between risks.
- Lack of management/ monitoring of IT risk.
- Lack of focus on change in the risk profile and emerging risks.
- The organization is not convinced of the value of risk management efforts resulting in a lack of commitment.
- The organization and responsibility is unclear between the Head of Risk Management and the risk owners

Work performed by the various control functions is uncoordinated.

- There is damaging competition/ professional rivalry between the Head of Risk Management and related functions e.g. Quality Management, Compliance and Internal Audit
- Poorly performed risk evaluations lacking documentation of the underlying criteria for the evaluations so that Executive Management loses confidence in the accuracy of the risk profile presented.
- Lack of quality assurance measures in respect of analyses/ evaluations.
- Lack of a holistic view to reporting where differing formats for risk evaluations hinder aggregation at a higher level.

XVIII. Risk Management Best Practices

- The taking of risk is a natural part of running any enterprise, but it is often not explicitly stated in the formulation of business decisions. The expression "risk" has often been exclusively associated with unwanted events, and risk management has been defined as analyzing and restricting the probability and impact of unwanted events. This is only one dimension of the total picture. Evaluating positive outcomes is just as important an element of ERM as evaluating the downside as ERM is concerned with the whole picture enterprise wide and evaluating risk strategy in relation to a portfolio of risks (The Institute of Internal Auditors, 2019).

- The objective of ERM is to maintain risk at an acceptable level and ensure the best balance possible between threats and opportunities — in line with the risk appetite and business strategy of the board and executive management. It is concerned with ensuring the achievement of goals as the enterprise develops and appropriate management of the organization's assets, including avoidance of losses as a result of unwanted events.
- A prerequisite for being able to exercise sound risk management is therefore that there are clearly defined goals at the strategic level, to which goals at other levels in the organization may be linked. In this way risk evaluations at all levels will be linked to a hierarchy of objectives which supports the enterprise's overall strategy.
- In practice this means ensuring the best possible basis for arriving at decisions at the various levels of the organization, so that the decisions made will support the overall objectives. Subsequently it is important to have a sound mechanism to ensure the achievement and monitoring of the decided activities.
- Risk management may be defined as systematic, coordinated, and proactive activities aimed at the evaluation and treatment of uncertainty and events which can impact the achievement of goals. This includes amongst other things the organization's ability to:
 - Influence the probability and positive or negative impact of events.
 - Understand/exploit correlation between various types of risk.
 - Monitor development of the risk profile over time.
 - Initiate activities which align the path of development with the required direction.
 - Build a culture which ensures the implementation of activities and leads to sound risk management.
- ERM means taking a holistic perspective, not just of the enterprise's status at a given moment, but also probable positive and negative developments in the future. In this way it becomes a tool for the balanced prioritization of resource utilization. For this reason, this work should also be harmonized with other management activities such as performance scorecards.
- It is important that defined risk appetite can be translated into operational practice. There should be a common thread going through an organization's various objectives, management limits, authorities, and scope of action which accords with the total risk appetite and strategy. In those organizations where it is difficult to quantify risk appetite, it is especially important to devise suitable guiding principles delineating who as a decision maker can decide what should be the acceptable level of risk based on the relevant qualitative evaluations.
- Risk management and decision making are interconnected. When making any major strategic decision, executive management should require a set of scenarios to be presented detailing impact and alternative actions, especially in the situation where there may be a high level of uncertainty.

XIX. Benefits of Risk Management

The following are some of the specific benefits of a preventative risk management program:

- See risks that are not apparent. Many of the real risks facing an organization cannot be gleaned from a textbook. A comprehensive preventative risk management program leverages a team of experts to identify and provide a deeper understanding of all types of risks (Osler, 2019).
- Provide insights and support to the Board of Directors. Board members may find it difficult to identify risks outside their areas of expertise and experience. Providing resources and advisory services to the Board and its committees charged with risk management will make them better able to discharge their duties.

- Get credit for cooperation. Many regulatory agencies have policies where they “give credit” to companies under investigation for having a compliance or a risk prevention program in place. While it is impossible to avoid risk and the manifestation of risk into potential problems, regulators want to see that an event is not due to a systemic breakdown and that the company has measures in place—such as proper leadership, training and certification—to prevent such activity.
- Build a better defense to class-actions. Plaintiffs in class actions and other downstream litigation often rely on their ability to convince triers of fact that the defendants have been negligent. This is harder to prove when the company can point to a preventative risk mitigation program that is in place to minimize these risks.
- Reduce business liability. Regulators and shareholders increasingly view litigation risk as a business liability. Reducing litigation risk upfront makes the company a more attractive investment.
- Frame regulatory issues. Preventative risk management programs provide greater insight into insurance, indemnity and liability issues and allow the company to better focus and structure its inquiry.

XX. Limitations to Risk Management

Organizations must accept that Risk Management is not going to solve all issues. Once implemented correctly, Risk Management will improve various activities and prepare us for future uncertainties, but there are limitations to Risk Management Schemes (Threatsandopportunities, 2019).

- Accidents occur no matter how much we prepare for them,
- It will not defer all risk from the organization,
- It aids decision making, it doesn't make decisions.

XXI. Key risk indicators

A key risk indicator (KRI) is a metric for measuring the likelihood of if an event and its consequence will exceed the organization's risk appetite. They can be quantified in terms of percentages, numbers, Rand values, time frames etc. The primary role of a KRI is to track trends over a period, these trends are then converted into early warning signals. Through the association of KRI's to risks contained within a risk register, the data gathered in a KRI's assists decision making process for the risk team by providing incite and actual measurable to based their risk management decisions on (Curasoftware, 2019).

KRIs are used to answer the question: “How is our risk profile changing and is it within our desired tolerance levels?” Within the Risk-based performance methodology, KRIs are/should be defined for all Key Risks, and included on the risk scorecard and scored on a 0-3 scale – see previous post on the Risk-based performance scoring methodology (Risk Based Performance Management, 2019).

Key Risk Indicators (KRIs) are useful tools for business lines managers, senior management and Boards to help monitor the level of risk taking in an activity or an organization. To business lines managers, they may help to signal a change in the level of risk exposure associated with specific processes and activities. To senior management, they reflect the level of risk exposure, use or stretch of resources and the effectiveness of key controls. To the Board, they can indicate whether the firm operates within the set risk appetite. Finally, for modelers, key risk indicators are a natural way of including the fourth element of AMA (Advanced Measurement Approach), the BEICF (Business Environment and Internal Control Factors), into operational risk capital (The Institute of Operational Risk, 2019).

Characteristics of Key Risk Indicators (KRI)

A good KRI should have at least the following characteristics:

- KRIs should be based on established Standards
- KRIs should be developed using consistent methodology
- KRIs should provide a clear understanding of the risk variables:
 - Potentiality (Can it occur?)
 - Probability (If it can occur, what is the likelihood?)
 - Timing (When is it most likely to occur? / How much time do we have before it occurs?)
 - Severity of the Risk (When it occurs, what is the \$ / % / # loss?)
- KRIs must be quantifiable (number, dollars, or percentages)
- KRIs must be easily applied and understood by the end users
- KRIs must provide trending analysis of the risk variables
- KRIs should validate or invalidate management decisions and actions
- KRIs should be timely, provide a simplified but complete view of the risk, and cost effective (Riskypops, 2019).

Lifecycle of Key Risk Indicators (KRI) (Figure 1.)

The key steps of a leading KRI program are represented below. The cycle starts with the identification of key risks to the organization, the risk that are significant enough to warrant active monitoring. To play a role in the prevention of risk, indicators must signal a rise in the level risk factors rather than counting the number of incidents that has happened. Like a KRI for car accidents is not the number of collisions (but it is rather speed, alcohol or fog), preventive KRIs capture elevated levels of what cause risks, rather than the incidents that have already occurred. Understanding the causes of the risks (step 2) is thus an essential prerequisite to the identification of leading key risk indicators. However, chances are the several existing performance and controls metrics already used in the organization can be reused and looked at in the perspective of leading KRIs (step 3). Deficient controls (red KCIs) are, by definition, indicators of elevated levels of risks. Similarly, poor performance (red KPIs) are, more often than not, announcing trouble (Chapelleconsulting, 2019). Once the existing metrics have be reviewed to assess whether they qualify also as KRIs, only the missing metrics need to be completed with new KRIs (step 4). KRI Design (step 5) relate to the structure of this particular form of reporting that are the risk indicators: data source and capture, frequency of reporting and thresholds, stakeholders to the process of collecting, reporting and acting on possible breaches, and governance rules in case of breaches (step 5). Finally, after a sometime (1 – 2 years) of using KRIs usage, it is advisable to test their effectiveness: have they helped to prevent any incidents? (step 6).

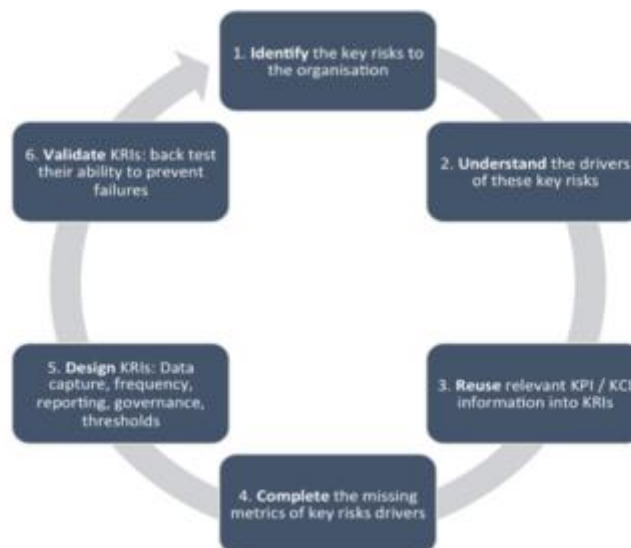


Figure 7. Source: (Chapelleconsulting, 2019).

KRI Processes

- KRI Identification
 - Identify existing metrics.
 - Assess gaps and improve metrics.
 - Identify KRIs via risk control self-assessment (RCSA)—interview business units.
 - Don't over rely on them; focus on indicators which track changes in the risk profile or the effectiveness of the control environment.
 - Concentrate on the significant risks and their causes and consider forward looking and historical indicators.
 - Consider absolute values and numbers, ratios, percentages, ageing, etc.
 - Data on KRIs should be collated on a systematic and consistent basis in order to be meaningful, e.g., on a monthly basis (Workiva, 2019).
- KRI selection
 - Select the KRIs that are measurable, meaningful and predictive (leading indicators).
 - Gather a good mix of leading and lagging indicators for effective risk management.
 - Don't select too many KRIs that:
 - Are too difficult to manage (track).
 - Might become unmanageable.
 - Select only the ones that provide useful information.
- Setting thresholds
 - Determine and validate trigger levels or thresholds.
 - Based on industry tolerance or internal acceptance.

- Board of directors should approve thresholds.
- Should coincide with risk appetite statement.
- KRI Tracking & Reporting
 - Periodic tracking of KRIs (monthly, weekly, depends on what the KRI represents).
 - KRIs should be reported regularly and escalation procedures should be in place (as part of the KRI framework) to ensure timely reporting to management and board.
 - Various KRIs will have different levels of escalation. When in doubt, escalate higher but don't dump too much information on management/board because they will get overwhelmed.
 - Reporting of KRIs to head of business units by KRI owners. Head of business units then reports into risk management. Risk management reports to risk board and when applicable, the full board.
 - This can help improve corporate governance structure.
- Risk Mitigation Plans
 - Risk mitigation plans (RMPs) should be set for High risk items.
 - Items with high severity or high frequency of occurrence need to have RMPs to mitigate risk and enhance controls.
 - Determine what is high risk by assessing control levels.
 - Track RMPs to ensure that controls are enhanced, and risk is mitigated. Report on RMPs to management/board and set target completion dates.

Methodology of Identification of Key Risk Indicators (KRI)

The approach for operational KRI identification consists of five steps:

Step 1: Definition of the perimeter of risks to manage. For an efficient operational risk management, the enterprise should focus on major risks. This kind of risk has a real and/or a significant potential impact on a company's financial statements. The significance level to decide whether a risk is major or not depends on each company (revenues, results, total asset, degree of sensitivity to risks, etc.). It should be set by the top management. Thus, major risks to be followed are those whose annual impact exceeds thresholds set in fact by management. The operational risk mapping serves as a guide to which managers can refer throughout the process of identifying company's major risks (Mouatassim&Ibenrissoul,2015).

Step 2: Identification of KRI dashboard recipients. The second step of the KRI definition process consists of the identification of the future receivers of dashboards. Indeed, appropriate indicators should be made available to the recipients according to their functions. Relevant good practices recommend sending to each operational manager key indicators related to risks within his scope of intervention. These indicators must be aggregated based on the hierarchy level. Furthermore, they need to be available for risk manager, if there is one in the company, for internal controllers and auditors to target their checks.

Step 3: Identification of actors that would participate in indicators' definition workshop. For a successful exercise of KRI identification, it is important to involve managers who would exploit indicators in the identification workshops. All operational managers who are responsible for managing and tracking major risks must be identified and invited to attend training sessions. The main goal of those sessions is to explain the objectives of the KRI system, the methodology for the indicators identification and thresholds setting up. The risk manager should also attend this training session in view of the important role he will play in the indicators and thresholds definition.

Step 4: Training of actors (designated in step 3) in KRIs identification methodology. Designated actors need to go through a training session dealing with identification of risk indicators process. This session should focus on:

- Definition of basic concepts: risk, major risk, key risk indicator, exposure indicator, proven risk indicator, environment indicator, specific indicator;
- Presentation of the objectives regarding the set-up of operational key risk indicators system;
- Presentation of the methodology for identification of key risk indicators and their thresholds (see step 5 below);
- Identification of people that would exploit these indicators but also those that would set up and control the KRI system;
- Presentation of the templates for KRI dashboards to produce.

Once the training session completed, a planning for holding indicators' identification workshop should be put in place.

Step 5: Holding the KRI identification and thresholds definition workshops in accordance with the predefined planning. As said above, there are two types of indicators namely, exposure indicators and proven risk indicators, calculated prior to or after risk occurrence. To identify exposure indicators, it is recommended to proceed as follows:

- Identify potential sources of each selected major risk;
- Determine the indicator that would quantify each identified source of risk.

As far as proven risk indicators are concerned, the approach for indicators identification is as follows:

- Identify consequences of each selected major risk;
- Define indicator that would quantify each identified consequence of risk.

However, it is possible to combine the two types of indicators for one risk in order to ensure effective monitoring before and after the occurrence of risk.

Mapping Risks to KRI

Managing risks is about managing the chain of:

- Detecting/predicting threats/opportunities
- Estimating the chance that they will happen (their probability)
- Controlling the impact/outcomes

Normally, we cannot map all these aspects of the risk in one KRI, so we will normally need 3 indicators:

- Indicator that would measure probability
- Indicator that would measure the impact
- Indicator that would measure action plan

For example, for such KRI as "Poor mentoring of employees" we would have: Time spend on mentoring per week, hours. This indicator estimates risk probability, the less hours one spends mentoring others, and the more likely the company will face this risk. Employee engagement index, %. This indicator helps to understand the impact of poor communication. Less mentoring means less engagement from the part of employees. Action plan: improve mentoring procedures; relevant indicator might be something like "Leadership training passed, hours." We need to teach managers a proper leadership paradigm that would include mentoring (BSC Designer, 2019).



Figure 8. Source: (BSC Designer, 2019).

Role of Technology in Effectively Measuring and Managing KRIs

Given the advances made by technology today, it is imperative to leverage it to look at different indicators in context of the risk data being collated for an organization. If the organization is already using a risk management system, then it has its risk and control assessment data, issue data, and can combine existing KRIs effectively (MetricStreams, 2019).

- Technology enables the measurement of different risk categories, metrics, and even occurrences. The system is not only for risks, it can also be used for asset classes, objectives, controls, processes, business entities etc. Once these are established, one can define thresholds (such as green, amber and red) – which represent rising and dropping indicators, both critical and non-critical. Reporting and dashboards make it easy to see critical areas for analyses, thresholds – breached or otherwise.
- Technology can be used to create a comprehensive story when KRI thresholds escalate. Automating KRIs to give them longer lives, track remedial action when KRIs are escalated, track follow ups – are some of the options available when technology is harnessed. Using technology also makes it easier to explain to regulators the actions performed, and the situations that mandated them, since it leaves an audit trail which reveals these details clearly.
- Risk management strategies can also be realized for specific, measurable, relevant and timely actions and responsibilities. Towards this objective, it is essential to understand KRI standards and measurement specifications. Furthermore, it is essential to determine the organization's analytics providers and the metrics consumers through various tools and resources.
- One of the biggest benefits of leveraging technology to manage KRIs is that it does away with manual efforts, which can be time consuming and cumbersome. Technology supports manual and automated data collation methods, enables easy definition of thresholds, and tracks issues and actions for breaches. It provides a single interface to define KRI, KPIs, KCI (Key Control Indicators) and risk appetites. It is possible to track metrics for causes, consequences and risks and these are easily accessible to personnel studying these within the organization. It is also easy to relate KRIs, KPIs and KCIs to anything in the organization's GRC library of content.

Benefits of Key Risk Indicators (KRI)

The constant measure of KRI can bring the following benefits to the organization:

- Provide an early warning: a proactive action can take place
- Provide a backward-looking view on risk events, so lesson can be learned by the past
- Provide an indication that the risk appetite and tolerance are reached
- Provide real time actionable intelligence to decision makers and risk managers (MetricStreams, 2019).

Management Challenges in Development of KRI Library

- Lack of standards and best practices—For better or for worse, the SMSIs look at the many operating methods and controls used successfully by other institutions. The SMSI often scales for its environment the more advanced management techniques of larger institutions. Until KRI practices mature and become time-tested, each institution will have to continue experimenting with different risk indicators to determine which are effective and manageable (The RMA Journal, 2019).
- Management Awareness—The control measures that get the most attention and support are those that senior management understand and expect. Because the concept of an enterprise-wide KRI library is still very new to the industry, many senior managers are unaware of its value, let alone its design, so they are hesitant to allocate scarce resources to develop such a program.
- Speed of change—Technology changes at an extremely rapid pace, so risks that may be embedded or inherent within a given technology today may increase or decrease with successive versions or developments. KRIs that are linked to a specific technology or even technology-centric process need to be routinely reevaluated any time that the underlying technology goes through a major revision.
- Control measures—Before effective KRIs can be designed and implemented, the institution must be able to clearly establish its internal control measures. An organization that is not confident in its control measures cannot build “status” measures around them. Fortunately, many institutions have gone through extensive exercises to document key control measures as a part of their compliance programs, particularly those subject to the Sarbanes-Oxley Act. These controls often serve as the foundation for determining active risk indicators.
- Lack of a process “decay” period—Some aspects of technology can be effectively monitored for subtle changes or degradation. Others defy monitoring. They can move very quickly from a stable state in which nothing is happening to one of dramatic change. For example, the lack of any computer viruses on the internal network can be routinely monitored, but a virulent computer virus that suddenly penetrates the network’s defenses can’t be measured by a KRI since the environment would go immediately from “stable” to “bad,” completely bypassing “trending toward bad.”
- Technology versus risk focus—People charged with implementing and maintaining the bank’s technology are, for the most part, focused on the technology itself and not necessarily the business risk associated with a potential failure of the technology. The development of technology-based KRIs is probably going to require the development of more mature communication channels between the subject matter experts regarding what could go wrong with the technology and what that would mean to the business.
- Technology versus process risk—Processes dependent on technology must include the potential failure of the technology as a risk. In failure scenarios, there is a gray area because the failure could be due to the technology itself or to how the technology is used. For instance, if the mis-configuration of an externally facing router exposes the bank’s network to the public Internet, is that a technology risk or a process risk? Many technology-centric KRIs may only make sense within the context of a full KRI library to cover all operational risk areas.

XXII. Practices in Kenya

Safaricom

Safaricom remains committed to robust risk management practices as an integral part of good management. This is demonstrated by the top down approach with the board taking overall responsibility of managing risk. Appropriate support toward risk management is given driving a positive risk culture across the organization. The board has overall responsibility for the company’s risk management and internal control systems. The Audit Committee reviews risk management initiatives including; Company risks and mitigating Controls, Safaricom compliance to requisite laws and regulations, and ethical environment. The Ethics Committee leads ethics and compliance initiatives and chaired by the CEO. It plays an oversight role and offers

strategic guidance on ethical matters in the business. The Chief Executive Officer responsible for prioritizing, aligning and arbitrating on risk management across the company while senior management are responsible for implementing appropriate risk management policies and procedures. The Risk Management Division is responsible for implementing the risk management programme in the business. The Director, Risk Management is a member of the Ethics Committee has a dotted reporting line to the Audit Committee. Safaricom has a clear framework for identifying and managing risk, both at an operational and strategic level. The risk identification and mitigation processes have been designed to be responsive to the everchanging environments in which we operate. The risk management framework that is aligned to the ISO 31000 allows Safaricom to identify, measure, manage and monitor strategic and operational risks across the business. The framework provides the management with a clear line of sight over risk to enable informed decision making. Safaricom continuously review the risk management framework which provides the foundation and organizational arrangements for identifying, treating, reporting, monitoring, reviewing and continually improving risk management throughout the organization (Safaricom, 2019).

KCB Group

KCB Group Plc is East Africa's largest commercial Bank that was established in 1896 in Kenya. Over the years, the Bank has grown and spread its wings into Tanzania, South Sudan, Uganda, Rwanda, Burundi and Ethiopia (Rep). Today KCB Group Plc has the largest branch network in the Region of 258 branches, 962 ATMs and over 16,600 merchants and agents offering banking services on a 24/7 basis in East Africa. This is complemented by mobile banking and internet banking services with a 24hour contact center services for the customers to get in touch with the Bank. The Bank has a wide network of correspondent relationships totaling over 200 banks across the globe and the customers are assured of a seamless facilitation of their international trade requirements wherever they are.

KCB embeds risk management and sustainability in all operations. Sustainability is about ensuring long term business success while contributing towards economic and social development, a healthy environment and a stable society. Put succinctly, sustainability is anchored in 3Ps i.e. Planet, People and Profit. Sustainability is creation of value for a wide range of stakeholders, including shareholders, employees, customers, suppliers, communities and Government, with consideration for the needs of future generation. Social sustainability through welfare of communities as well as our employees. Environmental sustainability through protection of natural resources. Financial stability of the financial institution and its clients, so that they continue to make long term contribution to development as well as Economic sustainability of projects and companies the financial institution finances. Sustainable banking is through the KCB SEMS (Social and Environmental Management System) Social and Environmental Management System is a framework that integrates social and environmental risk management into business process and aids the Financial Institution to avoid and manage loans with potential social and environmental risks by conducting due diligence prior to loan disbursement. KCB monitors risk and take pre-emptive action to adjust products, services and progress to ensure they do not expose the customers to undue risks (KCBgroup, 2019).

Equity Bank Group

Equity Group's pursuit of a unique business model and strategy to create resilience and manage headwinds of interest rate capping and challenging macroeconomic and business environment has delivered differentiated financial and business results that competitively positions the Group into an improving operating environment.

In pursuit of quality of income, the Group registered 38% of the total income contribution from diversified non-funded income streams. The strategy of focusing on non-funded income is building momentum with gross merchant commission growing at 30%.

Geographical and business diversification strategy continue to demonstrate the Group's ability to replicate the Kenyan successful model with non-banking and regional banking subsidiaries increasing their total assets to

26% of the Group's total assets, their deposits and loans contributing 24% and 25% respectively of the Group portfolio while their profit after tax contribution reached 15% of the Group profits.

Fintech innovation and digitization has powered rapid growth of merchant banking and diaspora banking. The cost structure of the bank has seen total cost grow by only 1% because of the shift of the business model from fixed cost infrastructure to variable cost 3rd party infrastructure and self-service model. 96% of all Group cash transactions are now happening outside the branch, primarily on mobile and agency network platforms. 93% of all successfully processed loans are now originated via mobile channels. Fintech innovation and digitization is delivering ease and convenience to customers explaining the new energy and growth momentum of intermediation characterized by growth in customer numbers and customer deposits. This strategy is contributing significantly to cost efficiency as the bank moves from fixed costs to customer self-service model and variable cost 3rd party infrastructure, lowering the staff and other operational costs. Focused and sustained investment in fintech innovation and digitization has resulted in operational efficiencies, cost optimization, customer convenience and ease of access and use of.

This has resulted in enhanced Group liquidity of 54% making the balance-sheet agile and flexible to market emerging opportunities associated with rapid regional growth. In pursuit of its ambition of shared prosperity, social and impact investments, the Group's spend through its corporate foundation has topped increased (Equitybankgroup, 2019).

East African Breweries Limited (EABL).

EABL is a regional leader in beverage alcohol with iconic brands across beer and spirits. The heritage since 1922 has enabled EABL understand consumers across the region, adopting world-class marketing and innovation skills to build powerful brands that play a positive role in society. EABL is structured into a market-based business model, applying country-specific strategies to meet consumer needs. The business model enables us to identify and act on consumer trends early. East Africa's vibrant beverage alcohol market has supported delivery of sustainable performance over the years.

East African Breweries Limited is committed to the highest standards of Corporate Governance and ethics. To ensure adherence to good governance and best practice, the company embedded internal policies and guidelines to guide activities involving our key stakeholders, namely employees, customers, suppliers, competitors, government and the community. The Company commissioned a rigorous Governance Audit, in a bid to continue supporting the visibility of the Corporate Governance agenda and to comply with the requirements of the Code of Corporate Governance promulgated by the Capital Market Authority.

EABL's elaborate approach to risk management is in line with Diageo's Global Risk Management Standard. On an annual basis, each business unit undertakes a 'blue sky' risk assessment. Thereafter, the top internal and external risks are ranked based on their likelihood of occurrence and their impact to the business. Action owners are then tasked with ensuring that robust mitigation plans are in place. These risks are reviewed every quarter by Business Units at the Risk Management Committee (RMC). The managers of the respective businesses in Kenya, Uganda and Tanzania as well as East Africa Maltings each chair the RMC in their business. In addition, EABL has a Control Assurance and Risk Management (CARM) framework in place covering all the major controls required for every function in the business to operate effectively, efficiently and in a compliant manner. As has been the case in previous years, the CARM process was refreshed with an assessment of key controls that are scoped for design and then tested (EABL, 2019).

XXIII. Conclusion

Researchers have found the relationship between robust risk management standards and business performance. Since the early 2000s, several industry and government bodies have expanded regulatory compliance rules that scrutinize companies' risk management plans, policies and procedures. In an increasing number of industries, boards of directors are required to review and report on the adequacy of enterprise risk management processes. As a result, risk analysis, internal audits and other means of risk assessment have

become major components of business strategy. Risk management standards have been developed by several organizations, including the National Institute of Standards and Technology and the ISO. These standards are designed to help organizations identify specific threats, assess unique vulnerabilities to determine their risk, identify ways to reduce these risks and then implement risk reduction efforts according to organizational strategy (TechTarget, 2019).

References

- [1]. BIA. (2019). *Risk management the what why and how*. Retrieved from <https://bia.ca/>
- [2]. BSC Designer. (2019). *Key risk indicators*. (2019). Retrieved from <https://bscdesigner.com/>
- [3]. CayenneConsulting. (2019). *What Kills Startups*. Retrieved from <https://www.caycon.com/>
- [4]. Chappelleconsulting. (2019). *Lifecycle of key risks indicators*. Retrieved from <http://chappelleconsulting.com/>
- [5]. CioIndex. (2019). *Risk management*. Retrieved from <https://cio-wiki.org/>
- [6]. Curasoftware. (2019). *Key risk indicator for enhancing risk management processes*. Retrieved from <https://www.curasoftware.com/>
- [7]. DBP Management. (2019). *5 ways to manage risk*. Retrieved from <http://www.dbpmanagement.com/>
- [8]. EABL. (2019). *Annual report 2018*. Retrieved from <https://www.eabl.com/>
- [9]. Equitybankgroup. (2019). *Financial results*. Retrieved from <https://www.equitybankgroup.com/>
- [10]. Financial Times. (2019). *Risk management*. Retrieved from <http://lexicon.ft.com/>
- [11]. IBM. (2019). *Risk management*. Retrieved from <https://www.ibm.com/>
- [12]. IIA Norge. (2019). *Guidance for the Risk Management Function*. Retrieved from <https://iia.no/>
- [13]. Kcbgroup. (2019). *Sustainability*. Retrieved from <https://kcbgroup.com/>
- [14]. Laboratory Equipment. (2019). *Risk management cycle*. Retrieved from <https://www.laboratoryequipment.com/>
- [15]. Marquette. (2019). *Risk management*. Retrieved from <https://www.marquette.edu/>
- [16]. MetricStreams. (2019). *Key Risk indicators ERM*. Retrieved from <https://www.metricstream.com/>
- [17]. Microsoft. (2019). *Risk management*. Retrieved from <https://docs.microsoft.com/>
- [18]. Mitre. (2019). *Risk management approach and plan*. Retrieved from <https://www.mitre.org/>
- [19]. Mouatassim, H., &Ibenrissoul, A. (2015). Proposal for an Implementation Methodology of Key Risk Indicators System: Case of Investment Management Process in Moroccan Asset Management Company. *Journal of Financial Risk Management*, **4**, 187-205. doi: 10.4236/jfrm.2015.43015.
- [20]. NCSC. (2019). *10 steps to cyber security*. Retrieved from <https://www.ncsc.gov.uk/>
- [21]. NCSU. (2019). *Factors to Consider in Risk Management*. <https://www.NCSU.edu/>
- [22]. Osler. (2019). *6 benefits of a risk management program*. Retrieved from <https://www.osler.com/>
- [23]. Programsuccess. (2019). *Risk management principles and definitions*. Retrieved from <https://programsuccess.wordpress.com/>
- [24]. Risk Based Performance Management. (2019). *Kpis Kris kcis are they different if so does it really matter*. Retrieved from <https://www.rbpm.co/>
- [25]. Riskyops. (2019). *Pure risk management training*. Retrieved from <http://riskyops.blogspot.com/>
- [26]. Safaricom. (2019). *Safaricom annual report*. Retrieved from <https://www.safaricom.co.ke/>
- [27]. TechTarget. (2019). *Risk management*. Retrieved from <https://searchcompliance.techtarget.com/>
- [28]. The Institute of Internal Auditors. (2019). *Very useful guidance on risk management best practices*. Retrieved from <https://iaonline.theiia.org/>
- [29]. The Institute of Operational Risk. (2019). *Key risk indicators*. Retrieved from <https://www.iior-institute.org/>
- [30]. The RMA Journal. (2019). *Developing Practical Key Risk Indicators for Operational Risks in Technology*. Retrieved from <https://cms.rmau.org/>
- [31]. TheIRM. (2019). *Risk management*. Retrieved from <https://www.theirm.org/>
- [32]. Threatsandopportunities. (2019). *Limitations to risk management*. Retrieved from <http://threatsandopportunities.com/>
- [33]. Workiva. (2019). *Operational risk key risk indicators*. Retrieved from <https://www.workiva.com/>