AJEMATES
African Journal of Educational Management, Teaching and Entrepreneurship Studies
VOL.10 (1), October-December, 2023 https://ajemates.org

RISK MANAGEMENT: A TOOL TO MITIGATE THE IMPACT OF UNCERTAIN EVENTS IN ANAMBRA STATE INTERNAL REVENUE SERVICE

Uzoka Obioma Agatha
obiomsy@gmail.com
Department of Business Education
Nwafor Orizu College of Education,
Nsugbe Anambra state

&

Johnson Onjero Joelin
onyero28andrew@gmail.com
Department of Business Administration
Nnamdi Azikiwe University.

ABSTRACT

Risk management has occupied an important place on the agenda of practitioners, academics and the business community and has been on the rise because it enhances organizational performance and creates value for shareholders. The main objective of this study is to examine the level of risk management implementation in the Anambra State Board of internal revenue. The paper examined types of risks and the antecedents of risk management implementation. It also investigated the moderating effect of top management support on the relationship between the antecedents and the level of risk management implementation. The research method was analytical and adopted a quantitative approach using secondary data. The need for more research on the importance of risk management in the mitigation of the impact of uncertain events government organisation has become imperative in view of the scarcity of research on risk management and the fact that risk management is still at its rudimentary stage in Nigeria.

Keywords: Risk Management; Mitigation; Impact; Uncertain Events; Internal Revenue Service.

Introduction

Risk is the possibility of something bad happening. Risk involves uncertainty about the effects/implications of an activity with respect to something that human's value, often focusing on negative and undesirable consequences. According to Azubuike (2018), risk is defined as the possibility of economic or financial losses or gains as a result of the uncertainty that comes with taking a specific course of action. Every human action (to varying degrees), every type of business, and every aspect of company management involves risk. These risks stem from a variety of sources, including financial uncertainties, legal liabilities, technology issues, strategic management errors, accidents and natural disasters. As a result, understanding the dynamics of risk control using various risk control techniques is critical for every organisation including government organisations, particularly income generating organisations, in order to minimize the impact of disaster and loses in the course of its performance. A set of techniques used by businesses to assess potential losses and take steps to mitigate or eliminate them is known as risk control (Adeoye, 2010).

As every organisation face new challenges every day as a result of a variety of factors including obstacles, competition, and other potential threats. Risk management approach is used by these organisations to identify, assess, and prepare for threats that can be physical or financial in nature and have the potential to affect their operations, aspirations, goals and objectives. With this, the organisation

will be able to effectively manage its operations so that returns can be maximized, losses minimised and general objectives achieved (Park and Yao 2015). In order to control these potential risks, innovative public organisations must identify and assess risks early. A risk management strategy could improve the ability to successfully manage all stages of the business management process (Grey, 2017).

The importance of risk management can never be over stressed. A successful risk management program helps an organization consider the full range of risks it faces. Risk cannot be avoided because it is said to surpass all human situations and it exists within public and private enterprises. Therefore, understanding risk dimensions and management is relevant for all organisations (Hardy 2010). The essence of risk management is to attain the most appreciable balance of opportunity and risk. This often means the organisation may in the process of pursuing a balance of opportunity and risk become exposed to new risks in adopting most preferred alternatives, hence the need for continuous awareness and proactive risk management practices (Vedpuriswar 2006). Risk management also examines the relationship between different types of business risks and the cascading impact they could have on an organization's strategic goals. This holistic approach to managing risk is sometimes described as enterprise risk management because of its emphasis on anticipating and understanding risk across an organization. In addition to a focus on internal and external risk threats, enterprise risk management (ERM) emphasizes the importance of managing *positive* risk. Positive risks are opportunities that could increase business value or, conversely, damage an organization if not taken, as the companies disrupted by Amazon, Netflix and other born-digital powerhouses will attest (Ogah, 2019).

Indeed, the aim of any risk management program is not to eliminate all risk but to preserve and add to overall enterprise value by making smart risk decisions. "We don't manage risks so we can have no risk. We manage risks so we know which risks are worth taking, which ones will get us to our goal, which ones have enough of a payout to even take them (Allan, Zil and Akler, 2016). Thus, a risk management program should be intertwined with organizational strategy. To link them, risk management leaders must first define the organization's risk appetite i.e., the amount of risk it is willing to accept to realize its objectives. Some risks will fit within the risk appetite and be accepted with no further action necessary. Others will be mitigated to reduce the potential negative effects, shared with or transferred to another party, or avoided altogether.

In Nigeria today, most public organisations do not have plan for risk management. This could be the reason there has been poor development of these organisations. In the ministry of internal revenue, one would rarely lay hand on policy plans for risk management. The ministry of internal revenue is the government owned organisation saddled with the responsibilities of revenue generation. According to Nwigbo (2018), the ministry of internal revenue is the government body saddled with the responsibility of general Supervision and control of collection of Personal Income Tax in in Nigeria. At the state level, it is called board of internal revenue. In Anambra state, the aim of board of internal revenue is to generally supervise and control of collection of personal income tax in the state, supervise and collect Internally Generated Revenue (IGR) in the State,

ensure accountability for all revenue collected in the State. Collation, compilation and publication of State revenue collection returns. For effective performance of this organisation, there is for effective risk management plan. Adoption of effective risk management plan is very crucial to the performance of the Board of internal revenue. Hence the need for assessment risk management tool for the mitigation of the the impact of uncertain events in Anambra State internal revenue service.

Statement of the Problem

Public Sector entities are often characterized with different categories of risk, arising as a result of both internal and external factors such as failure of contractors or Government agencies to provide services as required, project delays, cost overruns, inadequate quality standards, delay or failed introduction of new technology, loss or misappropriation of fund through corruption, disruption from industrial action, protest, communal clashes, inconsistent programmed objectives, inadequate contingency plans, failure to innovate, economic changes, environmental damages among others. All of these risk factors among others threaten the corporate existence and effective service delivery of public sector entities.

Consequently, this has brought the subject of risk assessment in both government and private institution on the front burner, which has resulted to the development of several government legislations and reforms, such as the Sarbanes Oxley Act in the USA, the Basel II capital and the revised combined code in the U.K. as well as the code of corporate Governance for public companies (part E) in Nigeria among others, to minimize the risk of future major corporate failure via tighter regulation of internal control system . The effectiveness and efficiency of risk control and risk financing (risk management) seems to pose enormous challenges in various industry, public sector not exempted. Thus, the problems facing public entities in risk assessment as identified in this study are: the problem of an effective risk control measures; the problem of choosing an efficient risk financing measures and the challenge of an independent, objective and professional internal audit assurance regarding the effectiveness and efficiency of risk control and risk assessment. A conclusion that can be drawn from Anambra State board of internal revenue is that even though internal controls system are usually developed for risk assessment in the organization belonging to the central and local government subsystems of public finances, risk assessment techniques are not fully integrated and thus, not effective within the organizational operations. Also, there is dearth of empirical data at present, about the influences of risk management on the performance of Anambra State board of internal revenue. It is in an attempt to fill this gap that this study seeks to assess the effect of risk management on the performance of Anambra State board of internal revenue.

Objectives of the Study

The primary purpose of this study is to examine the impact of risk management on the performance of Anambra State board of internal revenue. Other specific objectives are:

1. To examine the impact of risk management on the performance of Anambra State board of internal revenue.
2. To find out the relationship between risk selection and financial performance of Anambra State board of internal revenue.

3. To measure the impact of risk management on Anambra State board of internal revenue.

Research Questions

The study is being guided by the following research questions:

1. What are the impacts of risk management on the performance of Anambra State board of internal revenue?
2. What are the relationships between risk selection and financial performance of Anambra State board of internal revenue?
3. What are the impact of risk management on Anambra State board of internal revenue

Important of risk management

Risk management has perhaps never been more important than it is now. The risks that modern organizations face have grown more complex, fuelled by the rapid pace of globalization. New risks are constantly emerging, often related to and generated by the now-pervasive use of digital technology. Climate change has been dubbed a "threat multiplier" by risk experts. A recent external risk that initially manifested itself as a supply chain issue at many companies -- the COVID-19 pandemic -- quickly evolved into an existential threat, affecting the health and safety of employees, the means of doing business, the ability to interact with customers and corporate reputations.

Businesses made rapid adjustments to the threats posed by the pandemic. But, going forward, they are grappling with novel risks, including the ongoing issue of how or whether to bring employees back to the office, what can be done to make supply chains less vulnerable, inflation and the business and economic effects of the war in Ukraine.

In many companies, business executives and the board of directors are taking a fresh look at their risk management programs. Organizations are reassessing their risk exposure, examining risk processes and reconsidering who should be involved in risk management. Companies that currently take a reactive approach to risk management -- guarding against past risks and changing practices after a new risk causes harm -- are considering the competitive advantages of a more proactive approach. There is heightened interest in supporting business sustainability, resiliency and agility. Companies are also exploring how AI technologies and sophisticated GRC platforms can improve risk management.

Here's a primer on risk exposure and how it is calculated.

Financial vs. nonfinancial industries.

In discussions of risk management, many experts note that managing risk is a formal function at companies that are heavily regulated and have a risk-based business model. Banks and insurance companies, for example, have long had large risk departments typically headed by a chief risk officer (CRO), a title still relatively uncommon outside of the financial industry. Moreover, the risks that financial services companies face tend to be rooted in numbers and therefore can be quantified and effectively analyzed using known technology and mature methods. Risk scenarios in finance companies can be modeled with some precision. For other industries, risk tends to be more qualitative and therefore harder to manage, increasing the need for a deliberate, thorough and consistent approach to risk management, said Gartner analyst Matt Shinkman, who leads the consulting firm's enterprise risk management and audit practices. "Enterprise risk management programs aim

to help these companies be as smart as they can be about managing risk," he added.

Traditional risk management vs. enterprise risk management

Traditional risk management often gets a bad rap these days compared to enterprise risk management. Both approaches aim to mitigate risks that could harm organizations. Both buy insurance to protect against a range of risks -- from losses due to fire and theft to cyber liability. Both adhere to guidance provided by the major standards bodies. But traditional risk management, experts argue, lacks the mindset and mechanisms required to understand risk as an integral part of enterprise strategy and performance.

For many companies, "risk is a dirty four-letter word -- and that's unfortunate," said Forrester's Valente. "In ERM, risk is looked at as a strategic enabler versus the cost of doing business."

"Siloed" vs. holistic is one of the big distinctions between the two approaches, according to Shinkman. In traditional risk management programs, for example, risk has typically been the job of the business leaders in charge of the units where the risk resides. For example, the CIO or CTO is responsible for IT risk, the CFO is responsible for financial risk, the COO for operational risk and so on. Departments and business units might have sophisticated systems in place to manage their various types of risks, Shinkman explained, but the company can still run into trouble by failing to see the relationships among risks or their cumulative impact on operations. Traditional risk management also tends to be reactive rather than proactive.

The pandemic is a great example of a risk issue that is very easy to ignore if you don't take a holistic, long-term strategic view of the kinds of risks that could hurt you as a company," Shinkman said. "A lot of companies will look back and say, 'You know, we should have known about this, or at least thought about the financial implications of something like this before it happened.'"

In enterprise risk management, managing risk is a collaborative, cross-functional and big-picture effort. An ERM team, which could be as small as five people, works with the business unit leaders and staff to debrief them, help them use the right tools to think through the risks, collate that information and present it to the organization's executive leadership and board. Having credibility with executives across the enterprise is a must for risk leaders of this ilk, Shinkman said.

These types of experts increasingly come from a consulting background or have a "consulting mindset," he said, and they possess a deep understanding of the mechanics of business. Unlike in traditional risk management, where the head of risk typically reports to the CFO, the heads of enterprise risk management teams -- whether they hold the chief risk officer title or some other title -- commonly report to the CEO, an acknowledgement that risk is part and parcel of business strategy.

In defining the chief risk officer role, Forrester makes a distinction between the "transactional CROs" typically found in traditional risk management programs and the "transformational CROs" who take an ERM approach. The former work at companies that see risk as a cost center and risk management as an insurance policy, according to Forrester. Transformational CROs, in the Forrester lexicon, are "customer-obsessed," Valente said. They focus on their company's brand reputation, understand the horizontal nature of risk and define ERM as the "proper amount of risk needed to grow," as Valente put it.

Risk averse is another trait of organizations with traditional risk

management programs. But as Valente noted, companies that define themselves as risk averse with a low risk appetite are sometimes off the mark in their risk assessments. "A lot of organizations think they have a low risk appetite, but do they have plans to grow? Are they launching new products? Is innovation important? All of these are growth strategies and not without risk," Valente said.

Risk management process

The risk management discipline has published many bodies of knowledge that document ways for organizations to manage risk. One of the best-known resources is the ISO 31000 standard. Formally called ISO 31000:2018 Risk management -- Guidelines, it was developed by the International Organization for Standardization, a standards body commonly known as ISO. ISO 31000 outlines a risk management process that can be used by any type of entity and includes the following steps for identifying, assessing and managing risks:

1. Identify the risks faced by your organization.
2. Analyze the likelihood and possible impact of each one.
3. Evaluate and prioritize the risks based on business objectives.
4. Treat -- or respond to -- the risk conditions.
5. Monitor the results of risk controls and adjust as necessary.

These steps are straightforward, but risk management committees should not underestimate the work required to complete the process. For starters, it requires a solid understanding of what makes the organization tick. To obtain that, the ISO 31000 process also includes an upfront step to establish the scope of risk management efforts, the business context for them and a set of risk criteria. The end goal is to know how each identified risk relates to the maximum risk the organization is willing to accept and what actions should be taken to preserve and enhance organizational value.

When identifying risks, it is important to understand that, by definition, something is only a risk if it has a business impact, according to risk expert Greg Witte, a senior security engineer for Huntington Ingalls Industries and an architect of frameworks developed by the National Institute of Standards and Technology (NIST) on cybersecurity, privacy and workforce risks, among others. For example, the following four factors must be present for a negative risk scenario, according to guidance from NISTIR 8286A, a report on identifying cyber security risk in ERM initiatives that NIST published in 2021:

1. A valuable asset or resources that could be impacted.
2. A source of a threatening action that would act against the asset or resources.
3. A pre-existing condition or vulnerability that enables the threat source to act.
4. Some harmful impact that occurs from the threat source exploiting that vulnerability.

While the NIST criteria pertains to negative risks, similar processes can be applied to managing positive risks.

Top-down, bottom-up. In identifying risk scenarios that could impede or enhance an organization's objectives, many risk committees find it useful to take a top-down, bottom-up approach, Witte said. In the top-down exercise, leadership identifies the organization's mission-critical processes and works with internal and external stakeholders to determine the conditions that could impede them. The

bottom-up perspective starts with the threat sources -- earthquakes, economic downturns, cyber-attacks, etc. -- and considers their potential impact on critical assets.

The final task in the risk identification step is for organizations to record their findings in a risk register, which helps track the risks through the subsequent steps of the risk management process. An example of such a risk register can be found in the NISTIR 8286A report cited above.

Risk management standards and frameworks

As government and industry compliance rules have expanded over the past two decades, regulatory and board-level scrutiny of corporate risk management practices have also increased, making risk analysis, internal audits, risk assessments and other features of risk management a major component of business strategy. How can an organization put this all together?

The rigorously developed -- and evolving -- frameworks developed by the risk management field can help. Here is a sampling of them, starting with brief descriptions of the two most widely recognized frameworks, ISO 31000 and the COSO enterprise risk management framework offered by the Committee of Sponsoring Organizations of the Treadway Commission, better known as COSO:

- **COSO ERM framework.** Launched in 2004, the COSO framework was updated in 2017 to address the increasing complexity of ERM and highlight the importance of embedding risk considerations into business strategies and linking risk management and operational performance. It defines key concepts and principles of ERM, suggests a common ERM language and provides clear directions for managing risk. Developed by consulting firm PwC with input from COSO's five member organizations and external advisors, the updated framework is a set of 20 principles organized into five interrelated components:

1. Governance and culture.
2. Strategy and objective-setting.
3. Performance.
4. Review and revision.
5. Information, communication and reporting.

- **ISO 31000.** Released in 2009 and revised in 2018, the ISO standard includes a list of ERM principles, a framework to help organizations apply risk management mechanisms to operations, and the process detailed above for identifying, evaluating and mitigating risks. Developed by ISO's risk management technical committee with input from ISO national member bodies, ISO 31000:2018 is a shorter and more concise document than its predecessor and includes more strategic guidance on ERM. The newer version also emphasizes the important role of senior management in risk programs and the integration of risk management practices throughout the organization.
- **BS 31100.** The current version of this British Standard risk management code of practice was issued in 2021 and provides a process for implementing concepts described in ISO 31000:2018 -- including functions such as identifying, assessing and responding to risks and then reporting on and reviewing risk management activities.

Other frameworks that focus specifically on IT and cybersecurity risks are also available. They include NIST's Risk Management Framework, which details a process for integrating security, data privacy and cybersecurity supply chain risk management initiatives into the system development lifecycle, and the ISACA professional association's COBIT 2019, an information and technology governance

framework that supports IT risk management efforts.

Enterprises might also consider establishing customized frameworks for specific categories of risks. Carnegie Mellon University's enterprise risk management framework, for example, examines potential risks and opportunities based upon the following risk categories: reputation, life/health safety, financial, mission, operational and compliance/legal.

In addition, various risk maturity models can be used to benchmark risk management capabilities and assess their maturity levels. The most prominent one is the Risk and Insurance Management Society's Risk Maturity Model (RMM), which was developed in 2005 with software vendor Logic Manager and updated in 2022. The revamped RMM helps risk professionals assess their programs in five categories: strategy alignment; culture and accountability; risk management capabilities; risk governance; and analytics. Other risk maturity models are available from the Risk Management Association, consulting firm Investors in Risk Management and the Organisation for Economic Co-operation and Development's Forum on Tax Administration.

The three lines model developed by the Institute of Internal Auditors (IIA) offers another type of standardized approach to support governance and risk management initiatives. Originally called the three lines of defense before being renamed in 2020, the IIA's model outlines the different roles that business executives, risk and compliance managers and internal auditors should play in risk management efforts, with a governing body providing oversight and accountability.

Benefits and challenges of risk management

Effectively managing risks that could have a negative or positive impact on capital, earnings and operations brings many benefits. It also presents challenges, even for companies with mature GRC and risk management strategies.

Benefits of effective risk management include the following:

- Increased awareness of risk across the organization.
- More confidence in organizational objectives and goals because risk is factored into strategy.
- Better and more efficient compliance with regulatory and internal compliance mandates because compliance is coordinated.
- Improved operational efficiency through more consistent application of risk processes and controls.
- Improved workplace safety and security for employees and customers.
- A competitive differentiator in the marketplace.

The following are some of the challenges risk management teams should expect to encounter:

- Expenditures go up initially, as risk management programs can require expensive software and services.
- The increased emphasis on governance also requires business units to invest time and money to comply.
- Reaching consensus on the severity of risk and how to treat it can be a difficult and contentious exercise and sometimes lead to risk analysis paralysis.
- Demonstrating the value of risk management to executives without being able to give them hard numbers is difficult.

Building and implement a risk management plan

A risk management plan describes how an organization will manage risk. It lays out elements such as the organization's risk approach, the roles and responsibilities of risk management teams, resources that will be used in the risk management process and internal policies and procedures.

ISO 31000's overall seven-step process is a useful guide to follow for developing a plan and then implementing an ERM framework, according to Witte. Here is a more detailed rundown of its components:

1. **Communication and consultation.** Since raising risk awareness is an essential part of risk management, risk leaders must also develop a communication plan to convey the organization's risk policies and procedures to employees and relevant parties. This step sets the tone for risk decisions at every level. The audience includes anyone who has an interest in how the organization takes advantage of positive risks and minimizes negative ones.
2. **Establishing the scope and context.** This step requires defining both the organization's risk appetite and risk tolerance -- the latter is how much the risks associated with specific initiatives can vary from the overall risk appetite. Factors to consider here include business objectives, company culture, regulatory requirements and the political environment, among others.
3. **Risk identification.** This step defines the risk scenarios that could have a positive or negative impact on the organization's ability to conduct business. As noted above, the resulting list should be recorded in a risk register and kept up to date.
4. **Risk analysis.** The likelihood and impact of each risk is analyzed to help sort risks. Making a risk heat map can be useful here; also known as a *risk assessment matrix*, it provides a visual representation of the nature and impact of a company's risks. An employee calling in sick, for example, is a high-probability event that has little or no impact on most companies. An earthquake, depending on location, is an example of a low-probability risk event with high impact. The qualitative approach many organizations use to rate the likelihood and impact of risks might benefit from a more quantitative analysis. The FAIR Institute, a professional association that promotes the Factor Analysis of Information Risk framework for cyber-risk quantification, has examples of the latter approach.
5. **Risk evaluation.** Here is where organizations assess risks and decide how to respond to them through the following approaches:
   - Risk avoidance, when the organization seeks to eliminate, withdraw from or not be involved in the potential risk.
   - Risk mitigation, in which the organization takes actions to limit or optimize a risk.
   - Risk sharing or transfer, which involves contracting with a third party (e.g., an insurer) to bear some or all costs of a risk that might or might not occur.
   - Risk acceptance, when a risk falls within the organization's risk appetite and tolerance and is accepted without taking any risk reduction measures.
6. **Risk treatment.** This step involves applying the agreed-upon controls and processes and confirming they work as planned.
7. **Monitoring and review.** Are the controls working as intended? Can they be improved? Monitoring activities should measure performance and look for key risk indicators that might trigger a change in strategy.

Risk management best practices

A good starting point for any organization that aspires to follow risk management best practices is ISO 31000's nine principles of risk management. According to ISO, a risk management program should meet the following objectives:

- Create and protect value for the organization, as an overarching principle.
- Be integrated into overall organizational processes.
- Be systematic, structured and comprehensive.
- Be based on the best available information.
- Be tailored to individual projects.
- Account for human and cultural factors, including potential errors.
- Be transparent and all-inclusive.
- Be dynamic and adaptable to change.
- Be continuously monitored and improved upon.

Another best practice for the modern enterprise risk management program is to "digitally reform," said security consultant Dave Shackleford. This entails using AI and other advanced technologies to automate inefficient and ineffective manual processes. ERM and GRC platforms that include AI tools and other features are available from various risk management software vendors. Organizations can also take advantage of open source GRC tools and related resources.

Risk management limitations and examples of failures

Risk management failures are often chalked up to willful misconduct, gross recklessness or a series of unfortunate events no one could have predicted. But an examination of common risk management failures shows that risk management gone wrong is more often due to avoidable missteps -- and run-of-the-mill profit-chasing. Here is a rundown of some mistakes to avoid.

Poor governance. The tangled tale of Citibank accidentally paying off a $900 million loan, using its own money, to Revlon's lenders in 2020 when only a small interest payment was due shows how even the largest bank in the world can mess up risk management -- despite having updated policies for pandemic work conditions and multiple controls in place. While human error and clunky software were involved, a federal judge ruled that poor governance was the root cause, although an appeals court overturned an order that the bank wasn't entitled to refunds from the lenders. Nonetheless, two months after the erroneous payment, Citibank was fined $400 million by U.S. regulators for "longstanding" governance failures and agreed to overhaul its internal risk management, data governance and compliance controls.

Overemphasis on efficiency vs. resiliency. Greater efficiency can lead to bigger profits when all goes well. Doing things quicker, faster and cheaper by doing them the same way every time, however, can result in a lack of resiliency, as companies found out during the pandemic when supply chains broke down. "When we look at the nature of the world … things change all the time," said Forrester's Valente. "So, we have to understand that efficiency is great, but we also have to plan for all of the what-ifs."

Lack of transparency. The scandal involving the New York governor's office underreporting coronavirus-related deaths at nursing homes in the state during 2020 and 2021 is representative of a common failing in risk management. Hiding data, a lack of data and siloed data -- whether due to acts of commission or omission -- can cause transparency issues. Avoiding that requires an enterprise-wide risk

management strategy with common risk terminology, documented processes and centralized collection and management of key risk data.

Limitations of risk analysis techniques. Many risk analysis techniques, such as creating a risk prediction model or a risk simulation, require gathering large amounts of data. Extensive data collection can be expensive and is not guaranteed to be reliable. Furthermore, the use of data in decision-making processes can have poor outcomes if simple indicators are used to reflect complex risk situations. In addition, applying a decision intended for one small aspect of a project to the whole project can lead to inaccurate results.

Lack of risk analysis expertise. Software programs developed to simulate events that might negatively impact a company can be cost-effective, but they also require highly trained personnel to accurately understand the generated results.

Illusion of control. Risk models can give organizations the false belief that they can quantify and regulate every potential risk. This could cause an organization to neglect the possibility of novel or unexpected risks.

Risk management trends

The spotlight that was shined on risk management during the COVID-19 pandemic has driven many companies to not only reexamine their risk practices but also to explore new techniques, technologies and processes for managing risk. As a look at the trends that are reshaping risk management shows, the field is brimming with ideas.

More organizations are adopting a risk maturity model to evaluate their risk processes and better manage the interconnectedness of threats across the enterprise. They are looking anew at GRC platforms to integrate their risk management activities, manage policies, conduct risk assessments, identify gaps in regulatory compliance and automate internal audits, among other tasks. Newer GRC features that risk management experts said should be considered include the following:

- Analytics for geopolitical risks, natural disasters and other events.
- Social media monitoring to track changes in brand reputation.
- Security systems to assess the potential impact of data breaches and cyber-attacks.
- Third-party risk assessment tools to help strengthen supply chain risk management.

In addition to using risk management to avoid bad situations, more companies are looking to formalize how to manage positive risks to add business value.

They are also taking a fresh look at risk appetite statements. Traditionally used as a means to communicate with employees, investors and regulators, risk appetite statements are starting to be used more dynamically, replacing "check the box" compliance exercises with a more nuanced approach to risk scenarios. The caveat? A poorly worded risk appetite statement could hem in a company or be misinterpreted by regulators as condoning unacceptable risks.

More organizations are connecting their risk management initiatives and environmental, social and governance (ESG) programs, too. That's making sustainability risk management and efforts to address other kinds of ESG risks a higher priority for companies looking to make their operations more sustainable and ensure that they're acting in responsible and ethical ways.

Finally, while it's tough to make predictions -- especially about the future, as the adage goes tools for measuring and mitigating risks are getting better. Among the improvements? Internal and external

sensing tools that detect trending and emerging risks

Research Method

The research design adopted for the study is a descriptive survey design aimed at collecting information from the respondent based on their personal experiences on the impact of risk management on the performance of Anambra State Board of internal revenue. The population of the study was two hundred and ten (210) staff in Anambra State Board of internal revenue. A simple random sampling technique was used to select 200 teachers from 21 local government areas in Anambra State. Structured questionnaire was the instrument used for data collection. Two hundred copies of the questionnaires were distributed to the respondents who filled and then submitted. The researcher used statistical mean in analysing the data collected.

However, descriptive statistics and correlation analysis were used to analyse the data generated for the study

.

Presentation of Results

Data collected for this study are arranged based on the research questions and are presented in tables

Table 1: Descriptive Statistics

	Organizational Efficiency	Identify Risk	Risk Analysis	Evaluating Risk	Treat Risk	Monitor and Review
Mean	3.42	2.79	3.11	3.31	3.07	3.26
Std Dev	0.612	0.501	0.552	0.603	0.529	0.589

After calculating the means and standard deviations for each variable of the study, the highest mean value is risk evaluation (3.31), indicating that the main factor of risk management affecting organizational efficiency is risk identification while evaluating risk identification with the lowest mean value indicates that it has the least effect on organizational efficiency.

Table 2: Spearman's Correlation

	Organizational Efficiency	Identify Risk	Risk Analysis	Evaluating Risk	Treat Risk	Monitor and Review
Organizational Efficiency	1					
Identify Risk	0.138	1				
Risk Analysis	0.542	0.231	1			
Evaluating Risk	0.761	0.315	0.401	1		
Treat Risk	0.491	0.102	0.112	0.477	1	
Monitor and Review	0.550	0.221	0.247	0.098	0.192	1

The correlation analysis table in table 2 above suggest that this risk management process has relationship with organizational efficiency. Evidently, evaluations of risk show a very high and positive relationship with organizational efficiency, and this

could support pour findings in table 1. Similarly, identification of risk shows a very low and positive relationship with organizational efficiency.

Regression Analysis

Regression is a statistical technique used in accounting, making investments, financial reporting, and other disciplines to determine the strength and character of a relationship between a single dependent variable and a set of other variables known as independent variables. Table 3, 4, and 5 below summarizes the regression output for the influence of risk management on organizational efficiency in Nigeria which includes the Model Summary, Anova table, and Table of variable coefficient.

Table 3: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.960[a]	.923	.909	.04949

a. Predictors: (Constant), OF, IR, RA, ER, TR, MR

Table 4: ANOVA

ɔdel	Sum of Squares	df	Mean Square	F	Sig.
Regression	.496	1	.496	1771.43	.000[b]
Residual	.042	509	.000082		
Total	.537	510			

a. Dependent Variable: Organizational Efficiency

b. Predictors: (Constant), OF, IR, RA, ER, TR, MR

Table 5: Coefficients

Model	standardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
	ıstant) 6.622 .274			24.130	.000
	.114 .065		.216	1.737 2.962	.087
	.391 .132		.441	.3032	.000
	.114 .376		.207		.027
	.061 .105		.073	0.583	.045
	.228 .104		.177	2.204	.029
a. Dependent Variable: Organizational Efficiency					

The result of the regression analysis is summarized above, table 5 specifically shows that the model for risk management and organizational efficiency anambra state

board of internal revenue $= \mathbf{6.622} + \mathbf{0.114}(\mathbf{IR}) + \mathbf{0.391}(\mathbf{RA}) + \mathbf{0.114}(\mathbf{ER}) + \mathbf{0.61}(\mathbf{TR}) + \mathbf{0.228}(\mathbf{MR}) + \mu \ldots \ldots \ldots \ldots . (\mathbf{3})$ This reveals that risk analysis, evaluation of risk, treatment of risk, monitoring, and review of risk has a statistically significant positive effect on organizational efficiency at a 5% level of significance. However, identification of risk was not statistically significant at a 5% level of significance, hence it does not affect organizational efficiency.

Discussion of Findings

Anambra state of board of internal revenue is still reluctant when it comes to risk management, however for this study we outlined various risk management processes organizations should be able to effect in other to have organizational efficiency. The response from the respondents suggests that most of these organizations believed that evaluation of risk is a more important factor that affects organizational efficiency this is evident from its mean value (3.31) recorded in table 1. Secondly, the result of the correlation coefficient shows that all the risk management process is correlated with organizational efficiency and as such should be taken into consideration by organizations. The result of the regression analysis indicates that risk analysis, evaluation of risk, treatment of risk, monitoring, and review of risk has a statistically significant positive effect on organizational efficiency at a 5% level of significance. This implies that an increase in risk management will cause a corresponding increase in organizational efficiency.

Conclusion

From the findings of this research work, it can be deduced that fraud and forgeries in Anambra State Board of Internal revenue constitute a risk factor to their performance and is therefore playing an adverse role in its activities. It was also discovered that among the various types of risk confronting government organisation's performance, operations risk and credit risk are the commonest. These risks revolve around the activities of the management and workers in the organisation. However, the study showed that some risk management techniques put in place have been able to check or curb the various operational risks.

Recommendations

Based on the above, it is therefore recommended among other things that:

1. Apart from the operational risk as a result of human error or inefficiency, there are still other types of risk that should be paid attention to. The one that stood out is the credit risk which is still having adverse effect on the performance of the board of internal revenue
2. Nigerian government should strengthen the legal framework for the enforcement of taxation system.
3. Every government organisation especially the board of internal revenue should update its infrastructure so as to curb the system risk confronting the Nigerian banks. This would also prevent system failure.

REFERENCES

Azubuike (2018), Risk Management in public organisation in Nigeria. Owerri: Bon Publishers Ltd.

Nwankwo G.O (1991). Bank Management, Principle and Practice, Lagos: Malt House Press Ltd.

Nzotta M.S (2002). Corporate Financial Decisions, Owerri: Oliverson Industrial Publishers.

Ogunleye R.W (2001). "Sensitivity of Bank Stock Returns to Market and interest Rate Risks: An empirical investigation" NDIC, Quarterly Review, Vol.11 N01-2 pp57-77 June.

Olowe R.A (1998). Financial Management: Concepts, Analysis and Capital Investments, Lagos: Brierly Jones Nig Ltd.

Owualla S.I (2000). Principles of Financial Management, Lagos: G. Mag Investment Ltd.

Pandey, I.M (2004). Financial Management New Delhi: Vikas Publishing House. PVT.

Redja G.C (2006). Principles of Risk Management and Insurance, London: New- House Publisher Inc.

Soludo (2007). "Financial System Strategy 2020- The Next Development Threshold". A text of speech delivered at the Nigeria Television Authority 2nd National Lecture Series, held in Abuja.