



## Management of Operational Risks among Financial Institutions: Implications on Performance

Yomi Israel Aremu

Department of Accounting

Michael Okpara University of Agriculture, Umudike

### Publication Process

### Date

Received

April 01, 2019

Accepted

April 28, 2019

Published

July 29, 2019

### ABSTRACT

*This research work explored operational risk management among financial institutions in Nigeria and its implication on performance. This research work focused adherently on developing a framework for mitigating operational risks among financial institutions in Nigeria and exploring the implication of ORM on performance among financial institutions. Other business risk is well-understood, if not always managed effectively. However, the value of managing operational risk is only slowly gaining recognition in financial institutions in Nigeria. This work exposes success frameworks of international best practices which if financial institutions in Nigeria study and implement, will minimize the effect of operational risk on the performance of Nigerian financial institutions.*

**Keywords:** ORM; Operational Risk; Key Risk Indicators; Financial Institutions

### 1. Introduction

Operational risk is inherent in any business. It has been seen as 'the risk of a change in value caused by the fact that actual losses, incurred for inadequate or failed internal processes, people and systems, or from external events (including legal risk), differ from the expected losses' (RIMAN, 2006). Unlike other risks (credit risk, market risk, insurance risk), operational risks are not willingly incurred, nor are they revenue driven. They are undiversifiable and cannot be laid off which points to the fact that as far as the institutionalization of perfect systems, people, and processes is unattainable, operational risk cannot be fully eliminated.

Since operational risk cannot be eliminated completely, the need for its management has become a global concern among financial institutions. This concern is needful to keep losses within some level of risk tolerance (the amount of risk an entity is prepared to accept in pursuit of her corporate objectives). Operational risk is determined by balancing the costs of improvement in operations against the expected benefits in operations.

Two decades (from 1980 to the early 2000s) of globalization and deregulation (e.g. Big Bang (financial markets)), combined with the increased sophistication of financial services around the world, have introduced additional

complexities into the activities of banks, insurers and firms in general and therefore their risk profiles (Wikipedia, 2017).

Since mid-1990s, market risk and credit risk have been the subject of much debate and research, with the result that financial institutions have made significant progress in the identification, measurement and management of both these forms of risk. However, the near collapse of the U.S. financial system in September 2008 (Ivry, 2010) and the failure of SAT-3 in Nigeria is an indication that our ability to measure market and credit risk is far from perfect and eventually led to introduction of new regulatory requirements worldwide, including Basel III regulations for banks and Solvency II regulations for insurers.

The failure of Nigeria's terrestrial internet service provision, the South Atlantic 3/West Africa Submarine Cable, known as SAT-3 was declared as a major operational risk to the banks and other organizations with a high dependency on international and internet communications (Vanguard, 2009). The failure was said to have impacted over 70 percent of Nigeria's internet capacity, hence it rendered prostrate both public and private organizations, causing a great hindrance to performance. As at the time of the incidence, there was lack of operational risk management (ORM) in some organizations as stated by same report.

These reasons underscore the growing focus among banks and supervisors upon the identification, measurement and management of operational risk. The capacity to manage risk, and with it the appetite to take risk and make forward-looking choices, are key elements of the energy that drives the economic systems forward. Risk-taking is fundamental to companies' creation of value.

### Research Objectives

1. To develop a framework for mitigating operational risks among financial institutions in Nigeria.
2. To explore the implication of ORM on performance among financial institutions in Nigeria.

### Objectives of the Study

International trade has generally been regarded as the engine of growth for the global economy [Usman, 2011; Obadan & Okojie, 2014] and might be the catalyst required by small countries to achieve rapid growth (Arodoye & Iyoha, 2014). But in this 21<sup>st</sup> Century, there is a school of thought claiming that international trade propagates the under-development of poor nations due to unbalanced share of gains from trade that accumulates for industrialized countries. Therefore, this study focuses on the following objectives:

1. To examine the extent exportation has improved the economic growth of Nigeria
2. To measure the extent to which importation have influenced economic development in Nigeria
3. To determine the extent to which exportation can influence international trade.

### 2.1 Financial System and Operations

As stated by Robinson (2001) operations allude to producing the worth from holdings which are claimed by a business. The benefits might be either elusive or substantial. The operations include three principle administration goals which intend to expand the worth determined from the business possessions. These are producing salary, expanding business esteem and secure business wage (Robinson, 2001). For, example the items sold at higher costs are viewed as being profitable in the business portfolio.

The monetary arrangement of a nation and particularly its saving money framework is the primary system of activation of assets around profitable segments of a nation. This heading part has its establishment in the change of investment funds into speculation, a circumstance that helps maintain the development of a country. Nocco & Stulz (2006) notes, the money related framework assumes a focal part in fortifying the development of a country. From one perspective, money related frameworks assemble funds and aggregation, on the other, they advertise a productive assignment of capital. As stated by the author's position, great budgetary frameworks screen ventures

and push corporate administration on firms, guaranteeing that the acquired trusts have their most productive utilization. Essentially budgetary mediators additionally convert, differentiate and oversee different dangers in a manner that distinct savers couldn't do. To Rao (2012), the central significance of keeping money framework lies in the gigantic level of impact it places on different segments of the economy. Indeed, their disability reasons create an intrusion stream of credit to families and organizations, decreasing financing and utilization and in a few cases, heading for bankrupt organizations.

Consequently, poor bank administration not just brings liquidation to the organization by government offices, yet might in a few cases, it may have a negative impact on the trustworthiness of different banks bringing about systemic emergencies which brings about huge awkward nature in a nation's economy all in all (Rejda, 2011). Given this circumstance, it is important to have a proficient, intense and transparent keeping money framework, which attains an ideal distribution of assets, permitting one hand to boost benefits and the other helping monetary and social development of the country.

Notwithstanding, the above explanation is not generally so natural to actualize, particularly when the managing an account framework works in intricate markets that constrain to act in unsteady ranges where satisfactory danger administration is itself an approach to attain the vital goals of the foundation. Subsequently, the Basel Committee (2003) affirms that deregulation and globalization of budgetary administrations, coupled with the expanding refinement of monetary engineering frameworks build the intricacy of the exercises of banks and in this manner, their danger profiles.

Such explanations are reliable with those communicated by Shimpi (2001) who states; the movement of a bank is basically going out on a limb as each of its operations certainly or unequivocally holds doubt. The distinctive sizes of its operations are laid open to different sorts of danger which must be distinguished, measured and regulated, as the groundwork for setting the promoting methods and costs, bringing about a great mathematical statement between danger and prize (Shimpi, 2001). Subsequently, given the vicinity of danger in keeping money framework, its legitimate organization undoubtedly helps the making of quality for managing accounts.

## **2.2 Challenges in Banking Operations**

The principle issues emerge because of human blunder, lacking inner techniques, or frameworks disappointments as an aftereffect of outer occasions. This definition incorporates lawful danger, yet rejects key danger or business and reputational danger (Rifaut, 2006). Operational danger is characteristic in all exercises, items, frameworks and methodologies, and its starting points can be altered (methods, inside and outer duplicity, engineering, human assets, business hones, catastrophe, suppliers) (Rao, 2012). Money related action has developed exponentially. The development of money related undertakings in volume, as well as all the more significantly in multifaceted nature and amount of administrations has expanded. This sensation, around others, as the monetary outrages of the most recent decade has produced familiarity with the danger administration forms. Inside these procedures, dealing with a specific danger, which until as of late was not managed or measured or assessed legitimately (Nocco, 2006). Fiscal establishments have created propelled equations and proficient administration of operational dangers, permit them to quantify, and consequently attain better administration.

## **2.3 Overview of Operational Risk Management**

Operational danger administration alludes to a methodology which incorporates risk choice making, risk evaluation and the usage of the risk control that brings about moderation, acknowledgement or risk shirking (Basel Committee on Banking Supervision, 2003). For the fiscal foundations, the operational risk management necessity to be dealt with taking after the process to acknowledge survival and supportability. Feeble inner controls lead to misrepresentation and other exploitative exercises (Basel Committee on Banking Supervision, 1998). The capacity of operational danger administration is to acquire such exercises and to additionally ensure the respectability of the representatives of the association (Pereira, 2012). The operational risk is characterized by Ugoani (2012) as the

danger of misfortune coming about because of lack or fizzled methodologies, individuals, inward frameworks, or as an aftereffect of outer occasions. This definition is imparted by Yates (2011) who recognizes four classes of danger inside operational danger as follows:

- i. Personal: Misfortunes connected with deliberate violations of inward arrangements by the current staff or no more working at the organization.
- ii. Processes: Misfortunes that have been brought about by any lack, or absence of a technique. Misfortunes in this classification may come about because of errors in the monitoring details.
- iii. Systems: Misfortunes because of framework disappointments or current innovation.
- iv. External: Misfortunes coming about because of power of nature or as an aftereffect of occasions or circumstances brought on by outsiders.

As stated by Nocco & Stulz (2006), operational danger partnered by obstructions currently observing and regulating the positions taken, and in this way huge numbers of the bank risks are credited as stated by previously stated creators to deficient inside control disappointment. In this sense, the issue may be because administration was unable to regulate representatives who laid open the bank to misfortunes, or due to the confirmation of badly characterized strategies which created insolvency (Nocco & Stulz, 2006). In this respect, the Yazid, Hussin & Razali (2008) focuses out an itemized arrangement of how to distinguish operational hazard crosswise over diverse sorts of misfortune occasions, enveloping three levels. The principal level records seven sorts of occasions that are viewed as operational risk misfortune around those recognized are: internal misrepresentation (inward occasions), outside duplicity (outer occasions), work relations and security in the working environment, rehearses with clients' items and organizations, harm to physical possessions and interruption of business, framework disappointments and the execution, conveyance and procedure administration (Ugoani, 2012).

#### **2.4 Creating Operational Success**

Risk relies on introduction to future occasions; however, it is determined with presentation both the likelihood of the occasion and its effect assuming that it does happen. Risk administration is about recognizing and evaluating these risks, and choosing whether and how to react to them and relieve their effect (Nghlem, Coelli & Rao, 2007). Beyond the particular meaning of operational danger, what is imperative for saving money concerning operational danger is to have a procedure of operational danger administration. This methodology of examination is that the bank will guarantee great danger administration in the connection of universal benchmarks (Negash & Narayan, 2002). As stated by the Basel Committee, the essential standards for compelling management of an account supervision, operational risk administration alludes to dealing with the procedure of distinguishing proof, evaluation, following and control or scope operational danger (Menon, 2006). These four components reflected in extensive methodology to administration of dangers are the three mainstays of Basel II, and reports the best practices of operational risk management.

#### **2.5 Determinant Factors of Operational Risk**

As far as operational risk is concerned, the principle determinants of risks are the misfortune coming about because of fizzled inside techniques, disappointments in the execution of staff duties, framework disappointments, or else due to external reasons. In profundity, hazard administration is utilized before task usage (Yazid, Hussin & Razali, 2008). This is on account of it that needs adequate time for arrangements and venture arranging. Generally, disappointment to arrange helps various operational issues. Throughout the execution of tasks or courses of action, there should be intentional risks administration under the routine periods (Yates, 2011). This incorporates quality confirmation, wellbeing briefs, at-work preparation, execution surveys, and security checks.

## 2.6 Operational Risk Categories

*Official Basel II defines the following as the main categories of operational risk:*

1. The internal fraud: the typical example of internal fraud is the employee with an unlawful access to the accounts that achieve large sums of money (Wolf, 2008). This is obtainable in financial institutions that accept deposits.
2. The external fraud: External fraud refers to bribery and fraud performed by the people from outside of the organizations.
3. The events related to labor relations and workplace safety: Losses can also be linked to strikes or accidents that may occur with staff deriving from uncontrollable activities (Wolf, 2008).
4. The events related to customers, products and business practices: A typical example is bad practices in sales to customers, such as not giving any information about what they are selling, which can even be done with premeditation. This event is common in investment banks.
5. The damage to physical assets is those damages caused by natural events (such as floods, earthquakes or tsunamis), or simply those arising from disturbances, resulting in destruction and burning of shops and administrative, or due to accidents such as the explosion of an oil rig (Ugoani, 2012).

According to Stulz (2008), the business disruption and system failures: All the organizations comes across all the experienced situations where “the system hangs” and a bank can stay for hours unable to distribute cash (Slovic & Weber, 2002). The events related to the execution, delivery and process management, as may be errors that cause loss of checks in a bank.

Amongst these categories above, fraudulent activities have posed a major threat to Nigerian banks. “Perhaps, nowhere are frauds more serious and more pronounced than in the banking sector of the economy” Idolo (2010), especially in the Nigerian banking sector. Idolo went further to state that fraudulent activities are “one of the biggest single causes of bank failure and distress in the Nigerian banking system” (p. 2). More disturbing is the fact that not only outsiders, but bank employees engage in these fraudulent acts and in some cases, avoid detection, therefore inspiring others to participate in fraudulent activities as well (Onibudo, 2007). Nigeria Deposit Insurance Corporation (NDIC), an independent agency of the Federal Government of Nigeria in their publication assessed that around 1,914 bank employees of several banks were participating in fraudulent activities amid 1994 and 1996 (Udegbumam, 1998) and this has increased over the past few years considering the statistics of the losses that have been made from fraudulent activities in the Nigerian banks recently. As at the early 1980s, Ogwuma (1981) assessed that Nigerian banks were losing N1 million daily as a result of fraudulent activities. This assessment, compared to recent times, is very low as NDIC recorded several cases where Nigerian banks made losses amounting to N11.244 billion as a result of forgeries and other fraudulent activities (Kazeem and Ogbu, 2002). As recent as the 5th of August 2011, the Central Bank of Nigeria took ownership of three banks, namely Bank PHB, Afribank and Spring Bank as a result of the fraudulent activities amongst the executives and members of the boards (Komolafe and Kolawole, 2011).

## 2.7 Measures of Operational Risk

Table 2.7.1 Possible Measures of Operational Risk

Dimension	Measures
People	<ul style="list-style-type: none"> <li>✓ Job offers made to job offers accepted</li> <li>✓ Voluntary turnover</li> <li>✓ Loss of high-potential personnel to peer companies</li> </ul>
Processes	<ul style="list-style-type: none"> <li>✓ First time resolution rate for customer queries</li> <li>✓ Order fulfilment accuracy</li> <li>✓ Accounting Close cycle</li> <li>✓ Forecast completion cycle</li> <li>✓ Cash application match rate</li> </ul>

Customers	<ul style="list-style-type: none"> <li>✓ Average order frequency</li> <li>✓ Average number of products and services purchased</li> <li>✓ Number of negative interactions (disputes, complaints, service failures, etc.)</li> </ul>
Technology	<ul style="list-style-type: none"> <li>✓ Proportion of basic business transactions completed electronically</li> <li>✓ Number of distinct customers, supplier, and employee recordkeeping systems</li> <li>✓ Number of manual interventions in the purchase to pay process.</li> <li>✓ Online accessibility to full customer or supplier relationship information.</li> </ul>

Source: *Compiled by the Researcher*

A systematic approach to measuring this type of risk would require companies to routinely review many nonfinancial factors, such as the quality of corporate governance, employee management, and customer management processes; the company's use of technology; and its deployment of best practices. Numerous tools already available including the Balanced Scorecard, activity-based costing, driver-based forecasting, real options, Monte Carlo simulations, and scenario planning are designed to provide insights beyond pure financial results. They can add value if used appropriately, but few organizations have established a process for translating the information generated by these tools into an understanding of operational risk that then leads to better decision-making.

## 2.8 Challenges of Managing Operational Risk amongst Financial Institutions

Despite the industry's efforts to control operational risk, institutions still have much work to do. Risk Managers are struggling with questions like, 'How does the discipline add value to my organization?'; 'What does the advanced measurement approach's (AMA) modeling techniques say about the operational risks my firm is facing?'; 'What is the strategic role of operational risk my firm should adopt?'. Below are some challenges of ORM:

*Rising Costs of Compliance:* Development of an ORM model as part of a regulatory and economic capital framework is complex and takes time. There is a general agreement that the major ORM challenge is escalating cost of compliance.

*Access to Appropriate Information and Reporting:* Effective management of operational risk requires diverse information from a variety of sources-including, for example, risk reports, risk and control profiles, operational risk incidents, key risk indicators, risk heat maps, and rules and definitions for regulatory capital and economic capital reporting.

*Development of Loss Databases:* A well-structured operational risk framework requires development of business-line databases to capture loss events attributable to various categories of operational risk. Basel II specifically requires a minimum of three years of data for initial implementation and ultimately five years for the Advanced Measurement Approaches (AMA). The need for historical data (including external data) has been a cause for concern for many enterprises.

*Lack of Systematic Measurement of Operational Risk:* Many enterprises hold that their institutions are measuring operational risk. However, very few of them have been able to complete the Basel II quantification requirements, or yet to formalize the measurement process around the Basel II framework.

*Implementing ORM Systems:* Amid regulatory efforts to overhaul the industry's immunity to operational risk, and its implications on efficient financial intermediation, many organizations are looking to go beyond traditional soloed approaches and implement a consolidated ORM framework across entire value chain. Development of an ORM model as part of a regulatory and economic capital framework, however, is complex and takes time. Some banks may either still be struggling with the requirements of the "Sound Practices for ORM" BIS paper, which spells out how to introduce ORM principles, or may not yet have in place the required governance or framework. Factors like lack of understanding of upcoming technology regarding operational risk management, failure to get the top management to focus on the benefits of the program, improved productivity and quality, as well as on loss reduction,

and lack of meaningful and timely data across business unit and product lines make the implementation of an ORM system all the more formidable.

Tone at the Top: Effective risk management program starts with “The Tone at the Top”- driven by the top management and adhered by the bottom line. However, if bank’s top leaders perceive operational risk management solely as a regulatory mandate, rather than as an important means of enhancing competitiveness and performance, they may tend to be less supportive of such efforts. Management and the board must understand the importance of operational risk, demonstrate their support for its management, and designate an appropriate managing entity and framework - one that is part of the bank’s overall corporate governance framework.

## **2.9 Factors to be Considered by Nigerian Financial Institution in Developing a Framework for Operational Risk Management**

*There is no one-stop approach to ORM – as every firm follows a framework that is explicit to its own internal operating environment. When inquired about the standard ORM framework. In developing an analytical framework, there is no "standard" standard. Ultimately, the Operational risk framework should not merely be Basel-compliant; it should also provide the bank and other financial institutions with mechanisms for improving overall risk culture and behavior towards operational risk management. Understanding our risks should lead to better decision making and reflect in our performance”. As stated by (MetricStream, 2017), a robust operational risk management framework is made up of the following core components:*

1. **Governance:** It is the process by which the Board of Directors defines key objectives for the bank and oversees progress towards achieving those objectives. It defines overall operational risk culture in organization, and sets the tone as to how a bank implements and executes its operational risk management strategy. A successfully executed risk strategy often results in risk being firmly embedded in the vision, strategies, tools, and tactics of the organization. Governance sets the precedence for Strategy, Structure and Execution.
2. **Strategy:** A bank’s strategy for operational risk drives the other components within the management framework and provides clear guidance on risk appetite or tolerance, policies, and processes for day-today risk management.
3. **Appetite and Policy:** An ideal risk management process ensures that organizational behavior is driven by its risk appetite. Adopting an operational risk strategy aligned to risk appetite, leads to informed business and investment decisions.
4. **Clear Definition and Communication of Policy:** An organization’s top management must identify, assess, decide, implement, audit and supervise their strategic risks. There should be a strategic policy at the board level to focus on managing risk all levels and conscious efforts should be made to ensure that these policies are communicated at all levels and across entire value chain.
5. **Periodic Evaluations Based on Internal and External Changes:** An ideal risk management process puts improvement of risk performance on a competitive level with other important mission concerns – periodically evaluating the ORM performance goals in the light of internal and external factors. Depending upon the criticality of internal operating environment and key external factors, organization must review the strategic policies inside out.
6. **Structure:** When designing the operational risk management structure, the bank’s overall risk scenario should serve as a guideline. This includes initiatives like laying down a hierarchical structure that leverages current risk processes, developing risk measurement models to assess regulatory and economic capital, and allocating economic capital vis-à-vis the actual risk confronted. Centralized aggregation of operational risk information collected via various self-assessments across the organization, further, provides useful insight for the desired hierarchical structure. The implementation of these concepts allows risk to be handled consistently throughout the organization.

7. Execution: Once operational risk management structure is established by an organization, adequate procedures should be designed and implemented to ensure execution of and compliance with these policies at business line level. The first step includes identification and assessment of operational risk inherent in day-to-day processes of the bank. After assessment of inherent risk, target tolerance limit of risk should be established. This is commonly accomplished by calculating the probability/likelihood of materialization of risk, by considering the drivers or causes of the risk together with the assessment of its impact. The results of the risk assessment and quantification process enables management to compare the risks with its operational risk strategy and policies, identify those risk exposures that are unacceptable to the institution or are outside the institution's risk appetite, and select and prioritize appropriate mechanisms for mitigation.

## 2.10 Framework for ORM Solution

This solution offers industry's most advanced and comprehensive solution designed to meet Operational Risk needs of banks & financial services in Nigeria. The solution is based on an integrated Enterprise Compliance Platform (ECP) and International best practices for successfully managing risk and meeting regulatory requirements while lowering the associated costs that can otherwise be substantial. ECP, a proven infrastructure for building risk and compliance application, provides core modules and services to automate and streamline Operational Risk processes.

Its embedded best practices see expected loss as the amount a business should budget to cover its annual cost of operational failure while unexpected loss is the amount the business ought to reserve as capital.

This framework uniquely combines software and content to deliver ORM solutions content which helps define the scope of processes and sub-processes for which risk management needs to be performed and guides development of control and test libraries. It brings together all risk management related data - a reusable library of risks and their corresponding controls and assessments, results from individual assessments, key risk indicators, events such as losses and near-misses, issues and remediation plans - in a single solution. It also provides other intelligent and content driven features such access to training content from an expert community from within the solutions and integration of business processes with regulatory notifications and industry alerts. Key components of this solution framework for ORM would include:

*Risk Analysis and Risk Self-Assessment:* This provides a centralized risk framework to document all risks faced by the financial institutions in Nigeria. It supports risk assessment and computations based on configurable methodologies and algorithms giving an insight into organizations risk profile, enabling the risk managers to prioritize their response strategies for optimal risk/reward outcomes. Risk Control Self-Assessment (RCSA) forms a core part of the solution framework. Risk analysis and self-assessment capabilities enable organizations to document and evaluate their risk frameworks, including processes, risks, events, key risk indicators (KRI) and controls. Executive-level dashboard and reports provide visibility into the risk analysis, highlighting key risk metrics and policy compliance. Business process automation capabilities provide for real-time event escalation, automated risk processes and streamlined remediation of issues and action items.

*Control Design and Assessments:* Once the key risks are identified and prioritized, this operational risk framework will enable companies to define a set of controls that mitigate those risks. The solution also allows associated policy and procedure documents to be attached for reference. The system supports assessments based on predefined criteria and checklists and has a mechanism for scoring, tabulating and reporting results. The repository of all assessments with an easy search capability ensures that the users can check to see if a specific control was tested, access the assessment results and confirm whether it requires a remedial action plan.

*Loss Tracking and Key Risk Indicators (KRIs):* With loss event tracking, risk managers can track loss incidents and near misses, record amounts, and determine root causes and ownership. The provision of Statistical and trend analysis



capabilities enables end-users to track remedies and action plans. Key risk indicators (KRIs) provide capabilities for tracking risk metrics and thresholds, with automated notification when thresholds are breached.

*Issue Management and Remediation:* For issues arising from the assessment and auditing processes or from any other external events such as loss-events, scenario analysis or 'near-misses', this framework solution provides seamless issue management and remediation management capabilities. Once issues are identified, documented and prioritized, a systematic mechanism of investigation and remediation is set off by the underlying workflow and collaboration engine. The solution supports triggering automatic alerts and notifications to appropriate personnel for task assignments for investigation and remedial action.

*Internal Audit:* solution provides seamless integration with internal audit management for streamlining the auditing process in the organization. It provides the flexibility to manage a wide range of audit-related activities, data and processes to support risk management. It supports all types of audits, including internal audit, operational audit, financial statement audit, IT audits and quality audits. Advanced capabilities like built-in remediation workflows, time tracking, email-based notifications and alerts and offline functionality for conducting at remote field sites allow organizations to implement the industry best practices for efficient audit execution and ensure integration of the audit process with the risk and compliance management system.

*Reports and Dashboards:* The solution has the ability to track risk profiles, control ownership, assessment plans, remediation status, etc. on graphical charts that can be accessed globally and display real-time information. Ability to drill-down provides an easy way to access the data at finer levels of detail. In addition to pre-configured standard risk reports, the system provides flexibility by enabling stakeholders to configure ad-hoc or scheduled reports to view metrics on a variety of parameters such as by process, by business units, by status, etc. Quarterly and monthly trending analysis along with the ability to drill-down into each report and dashboard to see the underlying details enables risk managers and process owners to stay in constant touch with the ground reality and progress on risk management programs. Automated alerts for events such as exceptions and failures eliminate any surprises and make the process predictable.

## **2.11 Performance Benefits of ORM**

As ORM efforts mature, and gain both the support and the confidence of management, they are becoming increasingly valuable to the business. Perceived initially to support regulatory requirements, these efforts can be leveraged and aligned with business performance management. To be successful, however, such alignment must be based on a clear vision of the potential benefits. *Few of the benefits are discussed below*

*Identified and assessed key operational risk exposures:* ORM enables an organization to identify measure, monitor and control its inherent risk exposures of the business at all levels. Elements like Risk Assessment, Event Management, and Key Risk Indicator play an important role; enabling the organization to evaluate the risk controls, based on the identified inherent risk, and to measure the residual risk which remains after the implementation of controls.

*Clarified personal accountabilities, roles and responsibilities for managing operational risks:* Clear cut specification of roles and responsibilities of personnel regarding risk profile is an imperative part of implementing an integrated ORM framework. It not only streamlines the risk management process, but also allows risk managers to better incorporate accountability into the work culture of the organization.

*Evolved and enabled efficient allocation of operational risk capital:* With streamlined risk management process, efficient allocation and utilization of operational risk capital can be ensured.

*Consistent and timely operational risk management information and reporting capabilities:* Through the development of a well-tailored risk management strategy, a robust ORM system supports features like role-based

dashboards, control diagrams and scorecards that provide visibility into the ongoing risk management efforts and bring high-risk areas into focus.

*Sustained risk-smart workforce and environment:* Application of an ORM framework, in conjunction with related risk management activities, will support a cultural shift to a risk-smart workforce and environment in the organization. An essential element of a risk-smart environment is that it ensures that the organization has the capacity and tools to be innovative while recognizing and respecting the need to be prudent in protecting its interest.

*Ensured continuous risk management learning:* Most business units today acknowledge that continuous learning is fundamental to more informed and proactive decision-making; and a successful learning organization must align itself to the businesses it supports. To ensure continuous risk management learning, these business units are sharing their experience and best risk management practices - internally and across organizations. This supports innovation, capacity building and continuous improvement, and fosters an environment that motivates people to learn.

However, successfully navigating the road from compliance to value creation can be daunting without a roadmap and a clear vision. By taking a holistic approach to ORM an organization can significantly lower its risk profile and improve responsiveness to risk scenarios leading to strategic and operational benefits which will enhance performance.

### **3. Conclusion and Recommendation**

Risks associated with markets, liquidity, and credit are well-understood, if not always managed effectively. However, the value of managing operational risk is only slowly gaining recognition in the business world. The need to develop a systematic and rigorous approach to operational risk management is perhaps most widely understood in the financial services industry. One of the major elements in the Bank of International Settlements (BIS) New Basel Capital Accord, published in January 2001, defines operational risk as "the risk of direct or indirect loss resulting from inadequate or failed internal control processes, people, and systems or from external events." Andrew (2002) said, "We need to find ways for firms to provide a richer set of information about risk than is normally included in accounting standards." In other words, financial information is not enough to gauge a company's overall business risk. By tracking operational indicators, organizations can identify opportunities and threats before they affect financial performance. People, processes, customers, and technology illustrates some basic metrics for gauging operational risk. For example, if a company sees that the proportion of candidates accepting its job offers is falling, it can surmise that it is becoming a less attractive employer. The underlying reason could be that the company's reputation is deteriorating or that its competitors are offering better compensation packages. Early identification of this type of trend gives management time to react before the problem manifests itself in a labor shortage, decline in productivity, or increase in labor costs.

Finally, appropriate risk mitigation and internal controls procedures are established by business units such that residual risk is mitigated to the barest minimum. Regular reviews must be carried out, to analyze the control environment and test the effectiveness of implemented controls, thereby ensuring business operations are conducted within acceptable risk limits. Further, it is essential that the top management ensures consistent monitoring and controlling of operational risk, and that risk information is received by the appropriate people, on a timely basis, in a form and format that will aid in the monitoring and control. Operational risk metrics or "Key Risk Indicators" (KRIs) are established to ensure timely warning is received prior to the occurrence of an event. Key to effective KRIs lies in setting threshold at the acceptable level of risk. Execution and implementation of Operational Risk framework is key to setting up effective Operational Risk environment ensuring that business is conducted within appropriate risk tolerance limit.

## References

- Andrew, C. (2002, February 27). *Towards global financial reporting standards: a critical pillar in the international financial architecture*. Retrieved from Banks for International Settlements:  
<http://www.bis.org/speeches/sp020227.htm>
- Basel Committee on Banking Supervision (2003). *Sound Practices for the Management and Supervision of Operational Risk*, Bank for International Settlements, Basel, Switzerland, February 2003 [online]. Available at: <http://www.bis.org/publ/bcbs96.pdf> Accessed 24th July, 2017].
- Ivry, B. (2010, June 27). *Quoting Joshua Rosner as Stating 'It's not a liquidity problem, it's a valuation problem'*. Retrieved from Bloomberg:  
[https://www.bloomberg.com/apps/news?pid=20601170&refer=home&sid=aGT\\_xTYzbbQE](https://www.bloomberg.com/apps/news?pid=20601170&refer=home&sid=aGT_xTYzbbQE)
- Kazeem, O. and Ogbu, C. (2002), *Banks Record N11bn Fraud – NDIC*. Punch Newspapers, Lagos, September 2nd, Volume 19, Number 8596.
- Komolafe, B. and Kolawole, Y. (2011). *FG takes over Afribank, Bank PHB, Spring Bank*. August 5, 2011. [online]. Available from: <http://www.vanguardngr.com/2011/08/government-takes-over-three-rescued-banks/> [Accessed 28th June, 2017].
- Menon, N. (2006). *Non-Linearities in Returns to participating in Grameen Bank Programs*. *Journal of Development Studies*, Vol. 42, NO 8, 1379-1400. USA: Routledge.
- MetricStream. (2017, July 23). *Operational Risk Management (ORM) Framework in Banks and Financial Institutions*. Retrieved from Metricstream: [http://www.metricstream.com/solution\\_briefs/ORM.htm](http://www.metricstream.com/solution_briefs/ORM.htm)
- Negash, Z., Narayan, S.L., Amha, W., Abegaz, A. and Girmay, A. (2002). *Microfinance: Theory, Policy and Experience*. *Faculty of Business and Economics, Ethiopia: Mekelle University*.
- Nghlem, H. S., Coelli, T. and Rao, P. (2007). *The Welfare Effects of Microfinance in Vietnam: Empirical Results from a Quasi-Experimental Survey*. The 51st Annual Conference of the Australian Agriculture and Resources Economics Society 13-16 February 2007. Queenstown, New Zealand: Centre for Efficiency and Productivity Analysis.
- Nocco B. W. and Stulz, R. M. (2006). *Operational Risk*. *Journal of Applied Corporate Finance*, Volume 18 Number 4 A Morgan Stanley Publication, Fall, 2006.
- Onibudo, A.T. (2007), *Bank Frauds Problems and Solutions*. Unpublished B.Sc. Research Project, University of Benin, Nigeria.
- Pereira, M. V. F., McCoy, M. F. and Merrill, H. M. (2012). *Management Risk in the New Power Business*, Meril Energy, [www.google.com](http://www.google.com)
- Rao, S. (2012). *Credit Market Failures and Microfinance*. *International Journal of Research in Management & Technology (IJRMT)*, ISSN: 2249-9563.
- Rejda, G. E. (2011). *Introduction to risk management and insurance* (11th Ed.). Upper Saddle River, NJ: Prentice Hall.
- Rifaut, A. and Christophe, F. (2006). *Improving Operational Risk Management Systems*
- Robinson, S. M. (2001). *The Microfinance Revolution*. Washington, D.C: The World Bank. *Open Society Institute*.
- Shimpi, P. A. (2001). *Integrating corporate risk management*. New York, NY: Texere.

- Slovic, P., & Weber, E. U. (2002). Perception of risk posed by extreme events: Risk management strategies in an uncertain world. Available from:  
[http://www.ldeo.columbia.edu/chrr/documents/meetings/roundtable/white\\_papers/slovic\\_wp.pdf](http://www.ldeo.columbia.edu/chrr/documents/meetings/roundtable/white_papers/slovic_wp.pdf)  
[Accessed 21st January, 2014].
- Udegbonam, R. I. (1998). Bank Failure in Nigeria since Deregulation: Underlying Causes and Implication for Policy. *Benin Journal of Social Sciences*, Volume 6 & 8, Number 1 & 2.
- Ugoani, J. N. N. (2012). Poor credit risk management and bank failures in Nigeria. Available from:  
<http://ssrn.com/abstract=2185013> [Accessed 2nd April, 2014].
- Vanguard. (2009). *SAT-3: Operational risk to banks, organisations with high dependency on Internet*. Nigeria: Vanguard.
- Wikipedia (2017, June 20). *Operational Risk*. Retrieved from Wikipedia:  
[https://en.wikipedia.org/wiki/Operational\\_risk](https://en.wikipedia.org/wiki/Operational_risk)
- Wolf, R. (2008). The evolution of enterprise risk management. *The Actuary*, 5(3), 19-22.
- Yates, H. (2011). Insurance and Banking: The butterfly effect. *Risk Management Professional*, 3, 26-27.
- Yazid, A. S., Hussin, M. R., & Razali, A. R. (2008). A cross-sectional study on foreign exchange risk management by Malaysian manufacturers. *International Business Management Journal*, 2(2), 28-32.

**Copyrights:** The copyright for the published article is reserved by the author(s), with initial publication rights granted to the journal. This is an open-access article distributed under the terms and conditions of the [Creative Commons Attribution License](#).