MetricStream
GRC
SUMMIT 2013
MIDDLE EAST

Dr Abdulaziz Al-Terki
Head of Operational Risk, Burgan Bank, Kuwait

The Role of Operational Risk in an ERM Framework

The content of this article is based on a presentation made by Dr Abdulaziz Al-Terki, Head of Operational Risk, Burgan Bank, Kuwait, on the topic: 'The Role of Operational Risk in an ERM Framework,' at the MetricStream GRC Summit 2013 Middle East held in Dubai.

Introduction

Today, effective Risk Management is vital for any organization, owing to several factors including, changing regulatory, and legal requirements, ever-evolving technology, globalization, governance, expensive insurance costs, and the attitude of stakeholders. Operational risk, in the context of risk management, has become more significant now, than ever before. The need of the hour is for organizations to embed an effective Operational Risk Management (ORM) system in an ERM framework.

So, how do we define operational risk? According to Basel II[i], it is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. It includes legal risks, but excludes strategic and reputation risk.

Now, what is Enterprise Risk Management (ERM)[ii]? ERM is the process of planning, organizing, leading and controlling the activities of an organization to minimize the effort of risk on the organization's capital and earnings. By identifying and addressing risks and opportunities, organizations can protect and create value for stakeholders. ERM also equips management to effectively deal with potential future events that create uncertainty.

According to Risk Management Association (RMA):

- ERM, essential for any financial institution, encompasses all relevant risks.
- An ERM framework supports management competency to manage risks well, comprehensively, and with an understanding of the interrelationship among various risks.
- A successful institution incorporates a robust ERM capability as part of its culture by integrating what already exists to create a comprehensive and integrated view of the institution's risk profile in the context of its business strategy.

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Enterprise Risk Management-Integrated Framework[iii] published in 2004 defines ERM as a "process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." The COSO ERM Integrated Framework discusses key ERM principles and concepts, helps unify the ERM language across the organization, and provides clear direction and guidance for ERM.

Role of ERM

The role of ERM is vast. ERM keeps track of the risks that can arise from capital unavailability, political turmoil, legal and regulatory changes or changes in the physical environment of an organization. ERM also includes operational risks that are incurred by an organization's internal activities such as IT and business risks. Also, financial risk management that concerns the effective management of finances and the effects of external factors like availability of credit, foreign exchange rates, and interest rates, is a focus area of ERM. It also concerns compliance obligations around health and safety, consumer protection, data protection, employment practices, and regulatory mandates. Thus ERM assists an organization to achieve long-term objectives.

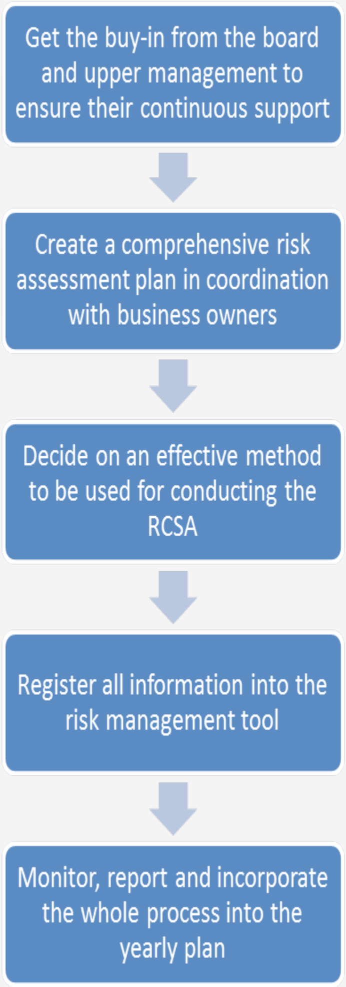
Operational Risk Management Framework (ORMF)

ORMF includes factors within the organization such as issue management, key risk indicators, control and self assessment, and loss of both external and internal data. This leads to an effective structuring, strategizing and execution of policies that result in better governance. An effective ORMF can be achieved through a process that involves governance structure, operational risk identification, assessment, measurement methodologies, policies, procedures, and processes for mitigating, controlling, monitoring, and reporting of operational risks.

Basel II that was intended to create an international standard for banking regulators to control how much capital banks need to put aside to guard against the different types of financial and operational risks banks face, lists three types of risks-credit risk, market risk, and operational risk. Various types of operational risks include system failure, IT security breaches, human error, regulatory breaches, and failure of service provider, server storms and project failures.

Role of ORM in an ERM Framework

A systematic approach is required to identify and manage all operational risks. The process begins with risk identification using workshops, surveys, and risk registers. Once identified, managers need to systematically and accurately assess risks in terms of impact and likelihood. After identification and assessment, risks are clustered under any of the four techniques to manage risk-avoidance, reduction, transfer and retention. For every risk category, a list of generic risks has to be elaborated in the risk register. The next step is to control risk. Risk management requires continuous monitoring and review of controls to evaluate its effectiveness in controling risk levels to avoid losses.



Get the buy-in from the board and upper management to ensure their continuous support

Create a comprehensive risk assessment plan in coordination with business owners

Decide on an effective method to be used for conducting the RCSA

Register all information into the risk management tool

Monitor, report and incorporate the whole process into the yearly plan

Five Steps to Risk Control Self Assessment (RCSA)

Understanding Risk Culture is vital for an effective ORM Program

Today, availability of newer technologies, organizational structures, market conditions, strategies and other factors are making it essential for enterprises to reassess their risk portfolio and reconfirm their risk appetite on regular basis. Risk appetite needs to be re-evaluated when the cost of mitigation forces higher tolerance for one or more risk conditions.

The focus should be on creating a risk culture, which concerns the behavior of an organization toward risk taking-cautious or aggressive, and policy compliance. The potential issues related to risk culture is that in many cases the organization's culture and policies are not aligned, resulting in potential non-compliance and unjustifiable risk. Thus it is essential for enterprises to adjust their policies in order to catch-up with ongoing changes in their culture.

Conclusion

To sum up, it is essential to understand the key elements of effective ORM within an ERM framework. An ORM governance structure needs to be developed using best practices and quality standards. This should be followed by effective operational risk identification, assessment, and measurement methodologies - both qualitative and quantitative. Unification of policies, procedures, and processes for mitigating and controlling operational risk is essential. At this level, decision makers and stakeholders should be informed about the effective monitoring and reporting of operational risks. It is important to adopt effective and simplified risk assessment techniques and connect risks to the strategic objectives of the organization. Finally, continuous guidance and awareness should be established to support the dissemination of risk management culture in the organization.

[i] Program on Designing Information Systems for Business and Basel II: http://www.cab.org.in/Lists/Knowledge%20Bank/Attachments/80/ITOperationalRisks-BaselII.pdf

[ii] Enterprise Risk Management: http://searchcio.techtarget.com/definition/enterprise-risk-management

[iii] Enterprise Risk Management-Integrated Framework: http://www.coso.org/documents/coso_erm_executivesummary.pdf

The content of this article is based on a presentation made by Dr Abdulaziz Al-Terki, Head of Operational Risk, Burgan Bank, Kuwait, on the topic: 'The Role of Operational Risk in ERM Framework,' at the MetricStream GRC Summit 2013 Middle East held in Dubai.

About MetricStream GRC Summit 2013 | Middle East
The MetricStream GRC Summit 2013 | Middle East was one of the largest and premier GRC Conferences in the Middle East that brought together Board Members, CEOs, GRC research analysts, subject matter experts and other business leaders from leading organizations across the Middle East & Africa and the rest of the world. Over 30 speakers, including GRC pundit and analyst, Michael Rasmussen, spearheaded the conversations at the Summit which witnessed sharing of ideas, best practices and challenges leading to drafting of actionable goals for the participants.
For more information, please visit www.grc-summit.com/mea2013.

Call us on: +971-5072-17139 | **Email**: grc-summit@metricstream.com