

2017 Enterprise Risk Management Symposium

April 20–21, 2017, New Orleans

A Refined Partnership Model for Effective Risk Management

By Zeinab Amin

A Refined Partnership Model for Effective Risk Management

Zeinab Amin, ASA, Ph.D.[1]

Abstract

Establishing organizational practices that support the development of a risk management culture across the organization is an essential step in the integration of risk management in day-to-day business activity. Several risk management models have been cited in the literature. These models describe how the risk committee, the central risk function in the organization, interacts with the rest of the organization. Each model offers numerous advantages to various stakeholders and suffers drawbacks with varying degrees. This paper looks at several risk management models, analyzes the pros and cons of every model and proposes a refinement of practice that improves operational efficiency and effectiveness. Alternative models will be compared based on the core elements of an efficient enterprise risk management program. We consider QInvest Bank as a good example of an effectively designed and adopted integrated risk management framework, a framework that makes risk management everyone's responsibility.

1. Introduction

The essential objective of any effective risk management program can be discerned from the definition of risk management given by the Institute of Risk Management (2002): "the process whereby organizations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities." To attain this goal, the organization has to have the ability to aggregate exposure metrics and risk tolerance at the enterprise level. There is a need for deep understanding that any business decision has to be considered holistically and a balance between risk and return has to be made.

A variety of risk management models can be used to describe the interactions between risk and assurance functions in the organization. Lam (2003) and Sweeting (2011) cited four models that can be used for risk management: the three lines of defense, the offense and defense, the policy and policing, and the partnership models. In addition to the three lines of defense model, some financial institutions outline a five lines of defense model to set the tone for the organization. All five models are based on the four core elements of risk management: risk identification, risk assessment, risk control and risk monitoring. However, they may vary in the assignment of roles and responsibilities to various units of the organization, whether risk is perceived in a holistic

[1] Correspondence can be sent to Zeinab Amin, Department of Mathematics and Actuarial Science, The American University in Cairo, P.O. Box 74, New Cairo 11835, Egypt, or via email at *zeinabha@aucegypt.edu*.

manner or in a silo approach, and the extent to which the risk management process is integrated with other areas of decision-making in the organization. The degree of focus on both the downside and upside of risk, and the level of communication and boundaries between various functions of the organization, also vary from one model to the other.

The paper is organized as follows. Sections 2 to 6 provide background information on the five risk management models: the three lines of defense, the five lines of defense, the offense and defense, the policy and policing, and the partnership models respectively. In Section 7, the effectiveness of these models is discussed by examining their characteristics, individual differences in terms of goals, and the enterprise risk management criteria used. Section 8 offers a good example of a financial institution where an effectively designed integrated risk management framework is adopted. The ninth section concludes the paper.

2. The Three Lines of Defense Model

This model suggests a hierarchy within the organization in managing risks. Various entities of the organization are classified into one of three lines of defense, each of which has a role in managing risk. The first line of defense is the operational line management, the line responsible for overseeing the daily operations in the organization. This is the function that owns and manages the risks their processes create. It is the function that identifies, assesses and mitigates risks. The risk management committee is the second line of defense. This is an independent function that oversees the risk and ensures risk owners manage the risk in accordance with an enterprisewide framework. It is the function that drafts policies, monitors their proper execution, ensures risk limit are adhered to, ensures the reliability of risk reporting and provides guidance to support the first line. The third line of defense is the audit. It is the function that determines if the process is in place and effective, the risk management framework is being implemented effectively as designed and consistently across the organization, and the internal controls developed are effective in meeting the needs of the organization. It is the function that provides independent assurance the other lines of defense are working effectively and gives sound advice if revisions of the program are needed.

The model provides a theoretical foundation for an effective risk and assurance framework. One of the main strengths of the model is that it sets a clear organized structure to ensure risk ownership, risk oversight and risk assurance are incorporated into the organization’s management system. It provides clear definitions of roles and responsibilities, provides clear and transparent assignment of oversight responsibilities to designated individuals, holds managers who are the risk owners accountable for managing risks, avoids any gaps in control and minimizes duplication of efforts.

3. The Five Lines of Defense Model

In addition to the operational line management, the risk management committee and the audit, the five lines of defense model identifies the board of directors and the executive management as additional lines of defense. The executive management is responsible for creating a risk culture where risk management is imperative to the organization and is everyone's responsibility. It is responsible for striking an appropriate balance between value creation opportunities and protection of the organization. It is the responsibility of the executive management to ensure other lines of defense are working effectively and alert the board of directors to any significant issues in a timely manner. The board of directors, as the elected representatives of the shareholders and other external constituents, serve as an oversight governing body and provide recommendations on any strategic issues as well as critical policy matters that can have a significant impact on risk management effectiveness.

Like the three lines of defense model, this model positions operational line management as the ultimate risk owners and hold them accountable for managing risks. It positions the risk management committee as a viable line of defense to ensure risk oversight and positions the audit as the provider of independent risk assurance and sound advice if revisions of the program are needed. In addition, this model allows for an enterprisewide risk oversight through the board of directors, who decide how risk is incorporated in strategy-setting and performance-measurement processes. It drives executive management to reinforce the message that managing risk is the expected role of everyone across the organization. Their overall ability to strike the appropriate balance between creating and protecting enterprise value determines the organization's ability to manage risk effectively.

4. The Offense and Defense Model

The offense and defense model suggests splitting various entities of the organization into the so-called offense and defense teams. The business units in the organization form the offense line while the risk management team forms the defense line. The critical issue in this model is not the division of entities; the critical issue revolves around how those entities perceive each other. If the two lines perceive each other as opposing teams with opposing goals, where one team has to lose the struggle for the other to win, conflicts will eventually escalate, inevitably creating a nonproductive and unhealthy business environment. Considerable skepticism may lead to defense dominance resulting in greater scrutiny and routine oversight processes and loss of opportunities as a result of moving too slowly. On the other hand, the two lines can perceive each other as one team with the same goal for which they hold themselves mutually accountable. Successful goal setting and effective communication is what will help the two groups work together effectively toward achieving their specific team goals and objectives.

5. The Policy and Policing Model

Like the offense and defense model, the policy and policing model involves two separate groups: A team comprised of the business units and a risk management team comprised of the risk management unit, the internal audit and the compliance unit. Lam (2003) describes the relationship between the two teams under this model as that of the government and citizenry. The risk management team establishes policies and limits the business line team has to abide by. Within these boundaries, no special approvals or management reviews are required, whereas those outside that limit are reviewed and the decision to approve or deny is made on a case-by-case basis based on the evidence provided. As long as they abide by the risk management policies, business units enjoy a high level of independence from the risk management team. Risks are handled in isolation with little consistency across different units as to how risks are identified, assessed and managed. While this independence reduces the confrontation that can often arise in the offense and defense model, it does not allow the risk management team to effectively fulfill its risk oversight role in continuously and consistently examining the risk management approaches across business units. Also, business managers are often unaware of how other risk exposures may be correlated to risks they encounter within their unit, which does not allow risks to be managed on an integrated basis. Business managers manage day-to-day operations in accordance with policies and procedures but are not engaged in the formation of risk strategies and policies.

The degree of independence between the two teams determines how knowledgeable business managers are about the organization's risk exposure, risk appetite, and the strategies and objectives the organization seeks to achieve; it also determines how well informed the risk management team is about risks constantly evolving across the organization.

6. The Partnership Model

In this model, risk management is fully integrated into the business, as opposed to being a defense line or a policing function. Business units and risk management team work as an integrated group; they streamline their activities within a common framework for managing risk; they prioritize their resources and effectively manage the key risks that have the highest potential impact on the organization. In this model, the whole group has common targets based upon the organization's growth priorities. They share their knowledge and expertise and guide decision-making to balance risk and return. Useful experiences are shared within the organization and the same mistakes are not repeated in similar situations. Modeling and measurement approaches for quantifying risks are implemented across all risk types at the enterprise level. The risk governance process of the organization is based on a clear definition of the organization's appetite of risk. Risk management is integrated into business performance analysis and incentive compensation. Effective communication and cultivation of a team culture are fundamental to the success of this model.

Sweeting (2011) points out the degree of collaboration between business units and the risk management team is an important issue that needs to be carefully resolved. The benefits of collaborative relations are clearly seen in reducing confrontation, creating a balance between risks and return, better prioritizing limited resources and producing aggregate metrics on risk exposure and risk appetite at the enterprise level. However, this program is not without its downside. The collaboration between the different lines of defense is seen as an obstacle that compromises the effectiveness of the risk management team in providing independent and objective assurance which risks are managed at acceptable levels.

7. The Effectiveness and Efficiency of Risk Management Models

Every enterprise faces a myriad of risks affecting different parts of the organization. From an enterprise risk management perspective, quantifying the impact on value should be the primary concern of managers. Among the most critical challenges for an enterprise risk management program is the ability to determine the amount of risk exposure in relation to the amount of risk the organization is willing to take as it strives to create value. Producing aggregate metrics on risk exposure and risk appetite at the enterprise level requires assumptions to be made about the interdependency of risks.

Except for the five lines of defense model and the partnership model, none of the three other models can be considered a value-centric approach to risk management. Although the risk management process in place may be considered solid, it is clearly silo based. Risks are identified at the unit level and decisions on mitigation are based on operational management's judgment in isolation, rather than on an integrated basis. Identifying and assessing risk at the first line of defense provides an incomplete risk profile as it does not capture the integrated impacts of multiple simultaneous risks. Business units conduct qualitative risk assessments developing simple risk status reports to the second line of defense. The second line in turn might receive redundant or conflicting information and might lack timely and robust information about exposures. It might also hinder their ability to quickly and effectively identify emerging risks. The organization may encounter risks for which the team is not adequately prepared. Failure to have an effective risk oversight role may ultimately obstruct the risk management team from assessing the organization's risk exposure and identifying its risk appetite. That degree of independence between different lines may not allow the risk management team to be involved in adding value by helping business managers define an optimal risk-return tradeoff as opposed to merely controlling risk. Also, that degree of independence may also hinder the team's progress toward linking incentive compensation to risk-adjusted performance, a key factor in developing a risk culture in the organization and cultivating awareness throughout the organizational structure.

In an effective enterprise risk management framework, all entities should join forces to identify a small number of key risks that have the largest potential impact on the organization. Focusing efforts and resources will ensure key risks are well understood and effectively managed and will

allow for better prioritization of limited resources. If risks are identified and risk limits for various risks are set independently without any significant coordination across silos, organizations might end up tracking an exhaustive huge list of risks rather than focusing on key potential risks that, if they occur, will affect achievement of an organization's objectives and increase the overall cost of mitigation. This additional cost could have been saved if information was shared and the risk appetite was defined at the enterprise level and cascaded downward through the organization to more granular levels.

Any risk management model that solely focuses on employing mitigation to lower the exposure and continuously reduces excessive risk-taking is criticized for putting too much emphasis on defense rather than exploiting opportunities to maximize returns. Focusing on the possibility of loss and the downside volatility of risk narrows the focus on the goal of optimizing risk-adjusted returns. The offense and defense model and the policy and policing model involve two separate groups: the business units in the organization and the risk management team. This division of entities may result in inefficiency and ineffectiveness if the relationship between the teams is strictly adversarial and teams operate in isolation, with one team exposing the organization to excessive risks in search of financial reward in the short term, and the other team being considerably skeptical, exerting excessive scrutiny and hence losing opportunities. Unless roles are coordinated in a manner that allows for sufficient cooperation between teams, and lines can effectively communicate and work in a collaborative manner rather than independently, these models will continue to be seen as confrontational and the risk function will continue to be visualized as a police function rather than a function that supports the business model. Restoring a balance between offense and defense in the risk management process is a key challenge for those models. Unless internal audits are partnering with operational management to seize risk opportunities and the link between risk and return is clearly understood, internal auditors may be viewed by operational managers as constantly stopping them from achieving their goals and the models will continue to raise controversial issue whether or not they are effective for risk management. This requires establishing clear communication protocols between the lines of defense and a holistic view of risk management. Both lines need a deep understanding of the importance of striking the right balance between risk and return and considering any business decision holistically.

To establish a healthy relationship between management units and the risk management team, Lam (2003) emphasizes the importance of maintaining a balance between effective corporate oversight and efficient business decisions, a balance that can only be achieved by integrating risk management into business management process.

8. QInvest

8.1 Background

QInvest is Qatar's leading investment bank with operations across the Middle East, Europe and Asia. The bank has authorized capital of US$1 billion, has the largest team of investment professionals in the Middle East and North Africa region, and has offices in Qatar, Saudi Arabia and Turkey, as well as affiliates in the United Kingdom and India. The bank is authorized by the Qatar Financial Centre Regulatory Authority (QFCRA).

8.2 Overview of the Risk Governance Structure

The bank's risk management process is an integral part of the organization's culture, and is embedded into the organization's practices. The board of directors, board risk and audit committee (BRAC), senior management, risk officers and line managers contribute to the effective groupwide risk management.

The risk governance structure is headed by the board of directors. The risk appetite and the risk strategy for the bank are developed at this level. The board of directors delegates the authority of monitoring the risks for different types of business activity of the bank to the next level, BRAC. The primary mandate of this board subcommittee is to assist the board in the effective discharge of its responsibilities for financial reporting, internal controls, risk management, compliance monitoring, and internal and external audit.

The day-to-day risk management functions are carried out by the identified control departments, which liaise with the chief executive officer for the daily management of specific risks. These control groups include the compliance, legal, finance and risk management (RMD) departments, and are manned by dedicated risk specialists in various disciplines to deal with the pertinent business risk exposures of the bank. In line with suitable governance policies, risk management and compliance departments have independent reporting lines to BRAC to allow the committee to provide its impartial view on the business activities taken by the group.

The risk appetite and risk tolerance set by the board of directors are cascaded across the institution and are taken into account in developing business goals and objectives. As part of an effective system of control, key management decisions are made by more than one individual, in the form of non-board management committees. The steering committee (STC) is the primary executive committee of the bank and is responsible for overseeing management of market risks, translating risk appetite and strategy directions into asset allocation guidelines, and reviewing the effectiveness of the operational risk management processes and procedures.

8.3 Risk Categories

The bank has exposure to various risks. These risks can be broadly classified into distinct categories for the purpose of calculating capital adequacy requirements. The categories are

credit, liquidity, market, operational and other (regulatory, legal and reputational). To better understand the risks facing the bank leading to improved control and risk management, we provide a broad description of these risks in the following subsections.

8.3.1 Credit Risk

Credit risk is the risk that an obligor or counterparty will fail to meet its contractual obligations in accordance with the agreed terms. For risk management reporting purposes, the bank considers and consolidates all elements of credit risk exposure (such as individual obligor exposure, business line exposure, country and economic sector risk, etc.).

The board of directors grants approval to the bank to engage in credit and investment related activities for approved products and is ultimately responsible for approving and periodically reviewing the credit and investment strategies and policies of the bank. The board of directors is also responsible for defining and setting the bank's overall levels of risk appetite, risk diversification and asset allocation strategies applicable to each Islamic financing instrument,[2] economic activity, geographical spread, currency and tenor.

The board of director delegates its responsibility of overall risk management to various board and senior management committees. The board investment committee (BIC) is responsible for evaluating and granting credit facilities and approving the bank's investment activities within authorized limits as set by the board and within the scope of activities approved by the QFCRA.

The STC evaluates credit and investment proposals and also exercises oversight on compliance with investment criteria, limits and investment procedures. The RMD is responsible for reviewing and scrutinizing the bank's risk management policies and procedures. The STC also reviews proposed guidelines on all risk and governance issues.

The RMD is responsible for the oversight and monitoring of the bank's credit risk, including:

- Formulating credit and investment policies in consultation with business units, covering credit and investment assessment, and risk reporting. RMD also facilitates establishment of the authorization structure for the approval and renewal of credit facilities. Approval and authorization limits are also allocated to executive management. Larger facilities require approval by BIC and/or the board of directors based on the authority limits structure of the bank.
- Reviewing and assessing credit and investment exposures before committing funds to investments or facilities.
- Exercising oversight for limiting concentrations of exposure to counterparties, countries and economic sectors.

[2] Islamic financing instruments include markup/fixed profit contracts (more akin to conventional financing), Sukuk (more akin to bonds) and profit and loss sharing contracts, which are based on participation by the financier in the project risk.

- Exercising oversight on ongoing monitoring of credit and investment exposures, market risk exposures and operational risk management.
- Providing advice, guidance and specialist skills to business units to promote best practices throughout the bank with regards to investment and credit risk management.

The RMD works alongside the investment department at all stages of a deal cycle from pre-investment and due diligence to exit and provides an independent review of every transaction. A fair evaluation of investments takes place every month with input from the investment department. Monthly updates of investments are reviewed by the STC. Regular audits of business units and group credit process are undertaken by internal audit.

8.3.2 Liquidity Risk

Liquidity risk is defined as the risk the bank will encounter difficulty in meeting obligations associated with financial liabilities settled by delivering cash or another financial asset. Liquidity risk arises because of the possibility the bank might be unable to meet its payment obligations when they fall due under both normal and stress circumstances.

The bank's approach to managing liquidity risk is to ensure, as much as possible, that it will always have sufficient liquidity to meet its funding requirements and liabilities when due, under both normal and stressed conditions, without incurring unacceptable losses or risking damage to the bank's reputation. The board of directors is responsible for approving the asset liability management (ALM) policy of the bank. In turn, the board may delegate part of its responsibilities to subcommittees and senior management. The board delegates the responsibilities of ALM to the STC. The STC is responsible for the overall asset and liability management function of the bank. The STC sets guidelines for the overall management of the liquidity and rate of return risk by recommending policies, setting limits and guidelines and monitoring the risk and liquidity profile of the bank on a regular basis. The STC also determines the borrowing and funding strategy of the bank.

8.3.3 Market Risk

Market risk is the risk of losses arising from movements in market prices. The objective of market risk management is to manage and control market risk exposures within acceptable parameters while optimizing the return on risk. As a matter of general policy, all trading positions on its assets and liabilities are being monitored on a daily basis by both business and control areas. Any material movements on the trading portfolios are addressed appropriately. All foreign exchange risk within the bank is transferred to the treasury. The bank seeks to manage currency risk by continually monitoring exchange rates. Overall authority for market risk is vested in the STC. RMD is responsible for the development of detailed risk management policies (subject to review and approval by the STC) and for the regular review of their implementation.

8.3.4 Operational Risk

Operational risk is the risk of loss arising from systems and control failures, fraud and human errors, which can result in financial loss, reputational damage, legal penalty or regulatory censure.

The bank manages operational risk through appropriate controls (such as segregation of duties, checks and balances, and the work of audit and compliance) and an operational risk management (ORM) framework. This framework adopts a three-pronged approach: self-analysis by each bank department through the operational risk self-assessment process, loss event/data reporting and issue tracking. Oversight of the ORM is exercised by RMD and STC.

QInvest has also developed a disaster recovery site within Qatar and a business continuity plan to facilitate the resumption and continuation of business in the event of a disaster impacting the bank's head office. The bank likewise transfers data outside Qatar into a repository facility in Singapore. This would enable the bank to re-build data in the event of an "in-country" disaster.

8.3.4 Other Risks (Regulatory, Legal and Reputational)

Regulatory or compliance risk is controlled through a framework of compliance policies and procedures that reflect the relevant legislations and QFCRA regulations. Legal risk is addressed through the effective use of internal and external legal advisers. Reputational risk is addressed by effective procedures around all areas concerning press and publicity releases, document production and website design.

9. Conclusions

This paper reviews some of the risk management models cited in the literature. As we analyze these models, we see they all offer numerous advantages to various stakeholders and that the level of success they can achieve depends on the ability to strike a balance between effective corporate oversight and efficient business decisions. One of the goals of this paper is to present a partnership model that involves all stakeholders and assists them to understand the challenges of balancing limited resources with risk targets, making the bank more resilient. We present an example of Qatar's leading investment bank, which has embarked on an ambitious program to quantify all their risks. The bank presents a value-based framework that provides the functional structure for an effective enterprise risk management partnership model—a framework that focuses on the presence and quality of the risk culture, maintains clear definitions of roles and responsibilities, provides clear and transparent assignment of oversight responsibilities to designated committees, and strikes an appropriate balance between value creation opportunities and protection of the organization.

The example we present demonstrates the framework is based on a collaborative relationship between the board of directors, board risk and audit committee, senior management, risk officers,

business segments, and internal and external risk experts in measuring, controlling and managing the overall risk of the bank. Clear communication protocols are established between these different entities. This framework emphasizes a balance between effective corporate oversight and efficient business decisions by integrating risk management into strategy-setting and business-management processes. This approach facilitates the appropriate top-down allocation of the risk appetite to individual limits for each business unit or risk type. It provides top management with the tools to trade off expected profits against risks for different types of business activity in the bank.

References

Institute of Risk Management. 2002. "A Risk Management Standard." *https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf*.

Lam, James. 2003. *Enterprise Risk Management: From Incentives to Controls*. Hoboken, N.J.: Wiley.

QInvest. 2014. "Annual Report 2014." *https://www.qinvest.com/sites/default/files/Annual%20Report%202014%20English.pdf*.

Segal, Sim. 2011. *Corporate Value of Enterprise Risk Management: The Next Step in Business Management*. Hoboken, N.J.: Wiley.

Sweeting, Paul. 2011. *Financial Enterprise Risk Management*. Cambridge: Cambridge University Press.