INTERNATIONAL JOURNAL OF INTERDISCIPLINARITY IN THEORY AND PRACTICE
ITPB - NR.: 11, YEAR: 2016 – (ISSN 2344 - 2409)

# RISK MANAGEMENT AND CONTROL: MODEL OF RISK CONTROL AND MANAGEMENT FOR CORPORATIONS AND FINANCIAL INSTITUTIONS

**Abdullah Rhoumah Alghwezi**[1]

**Abstract:** *It seems appropriate to begin the discussion of the place of risk and risk management in the financial sector with the two key issues: why risk matters and what approaches can be taken to mitigate the risks that are an integral part of the sector's product array.*

**Keywords:** Risk management, risk financial, management for corporation

## 1 INTRODUCTION

***Risk in Financial Services:***

Understanding these two issues leads to a greater appreciation of the nature of the challenge facing managers in the financial community. Specifically, it explains why managers wish to reduce risk, and approaches taken to mitigate something that is an inherent part of the financial services offered by these firms.

Why Does Risk Matter? According to standard economic theory, firm managers ought to maximize expected profits without regard to the variability of reported earnings. However, there is now a growing literature on the reasons for managerial concern over the volatility of financial performance, dating back at least to 1984.

Stulz was the first to offer a viable economic reason why firm managers might concern themselves with both expected profit and the variability around this value. Since that time a number of alternative theories and explanations have been offered to justify active risk management, with a recent review of the literature presenting four distinct rationales. These include:

(i) Managerial self-interest.
(ii) Tax effects.
(iii) The cost of financial distress.
(iv) Capital market imperfections In each case, the volatility of profit leads to a lower value to at least some of the firm's stakeholders.

In the first case, it is noted that managers have limited ability to diversify their investment in their own firm, due to limited wealth and the concentration of human capital returns in the firm they manage. This fosters risk aversion and a preference for stability. In the second case, it is noted that, with progressive tax schedules, the expected tax burden is reduced by reduced volatility in reported taxable income. The third and fourth explanations focus on the fact that a decline in profitability has a more than proportional impact on the firm's fortunes.

Financial distress is costly and the cost of external financing increases rapidly when firm viability is in question. Any one of these reasons is sufficient to motivate management to concern itself with risk and embark upon a careful assessment of both the level of risk associated with any financial product and potential risk mitigation techniques. In fact, the most well-known textbook in the field, Smith, Smithson, and Wilford (1995), devotes an entire chapter to motivating financial risk management as a value enhancing strategy using the arguments outlined above.

Risk Mitigation Approaches Accepting the notion that the volatility of performance has some negative impact on the value of the firm leads managers to consider risk mitigation strategies. There are three generic types:

(i) Risks can be eliminated or avoided by simple business practices.
(ii) Risks can be transferred to other participants.
(iii) Risks can be actively managed at the firm level. In the first of these cases, the practice of risk avoidance involves actions to reduce the chances of idiosyncratic losses by eliminating risks that are superfluous to the institution's business purpose.

Common risk avoidance actions, here, are underwriting standards, hedges or asset-liability matches, diversification, reinsurance or syndication, and due diligence investigation. In each case, the goal is to rid the firm of risks that are not essential to the financial service provided, or to absorb only the optimal quantity of a particular kind of risk.

What remains is some portion of systematic risk, and the unique risks that are integral to an institution's unique business franchise. In both of these cases, risk mitigation remains incomplete and could be

further enhanced. In the case of systematic risk, any systematic risk not required to do business can be minimized. Whether or not this is done is a business decision that can be clearly indicated to stockholders.

Likewise, in the case of operational risk, these risks of service provision - including fraud, oversight failure, lack of control, and managerial limitations - can be addressed.

Aggressive risk avoidance activities in both these areas will constrain risk, while reducing the profitability from the business activity. Accordingly, the level of effort focused on reducing these risks can be communicated to shareholders and cost-justified. There are also some risks that can be eliminated, or at least substantially reduced through the technique of risk transfer. Markets exist for the claims issued and/or assets created by many of these financial institutions. Individual market participants can buy or sell financial claims to diversify or concentrate the risk in their portfolios. To the extent that the financial risks of the assets created or held by the financial firm are understood by the market, they can be sold in the open market at their fair market value. If the institution has no comparative advantage in managing the attendant risk, there is no reason for the firm to absorb and/or manage such risks, rather than transfer them. In essence, there is no value-added associated with absorbing these risks at the firm level.

However, there is another class of assets or activities where the risk inherent in the activity must and should be absorbed by the firm. In these cases, risk management must be aggressive and good reasons exist for using further resources to manage firm level risk. These are financial assets or activities that have one or more of the following characteristics. First, the equity claimants, or others for whom the institution has a fiduciary interest, may own claims that cannot be traded or hedged easily by the investors themselves. For example, defined benefit pension plan participants can neither 6 trade their claims nor hedge them on an equivalent after-tax basis. A similar case can be made for policies of mutual insurance companies which are complex bundles of insurance and equity. Second, activities where the nature of the embedded risk may be complex and difficult to reveal to non-firm level interests. This is the case in institutions such as banks, which hold complex, illiquid and proprietary assets. Communication in such cases may be more difficult or expensive than hedging the underlying risk.

Moreover, revealing information about customers or clients may give competitors an undue advantage. Third, moral hazard may exist such that it is in the interest of stakeholders to require risk management as part of standard operating procedures. For example, providers of insurance, e.g., the FDIC, can insist that institutions with insured claims follow appropriate business policies. A fourth reason for institutional risk management is that it is central to its business purpose. An index fund invests in an index without hedging systematic risk. A security dealer engaged in proprietary trading and arbitrage will generally not be fully hedged. In all of the above circumstances, risk is absorbed and risk management activity requires the monitoring of business activity risk and return. This is part of the cost of doing business since it absorbs management attention.

The risks inherent in the industry are divided into the three categories we suggest, and the techniques of control as well as the goals of risk management for each group are enumerated. The communication challenge of informing stakeholders of the reasons for risk management activity is also reported for each risk category. With legitimate institutional risk management rationales defined and outlined, non-economic or redundant risk management practices can also be identified. These practices are associated with reducing risks through ill-considered hedges or through inappropriate diversification. Consider a recent example. During the 1980s a number of companies diversified into unrelated businesses. This was an attempt by their managements to break out of the cyclical nature of the profitability inherent in their basic franchise. Regardless of outcome, these investments could not help shareholders unless management had valuable skills in these areas. Clearly, without such skills, owners of the firms' stock could make such investments on their own

Operational risk is inherent in all banking products, activities, processes and systems, and the effective management of operational risk has always been a fundamental element of a bank's risk management programme.

As a result, sound operational risk management is a reflection of the effectiveness of the board and senior management in administering its portfolio of products, activities, processes, and systems

Risk management generally encompasses the process of identifying risks to the bank, measuring exposures to those risks (where possible), ensuring that an effective capital planning and monitoring programme is in place, monitoring risk exposures and corresponding capital needs on an ongoing basis, taking steps to control or mitigate risk exposures and reporting to senior management and the board on the bank's risk exposures and capital positions.

The operational risk governance practices adopted in an increasing number of banks. Common industry practice for sound operational risk governance often relies on three lines of defence:

(i) Business line management.
(ii) An independent corporate operational risk management function.
(iii) An independent review.

Depending on the bank's nature, size and complexity, and the risk profile of a bank's activities, the degree of formality of how these three lines of defence are implemented will vary. In all cases, however, a bank's operational risk governance function should be fully integrated into the bank's overall risk management governance structure.

In the industry practice, the first line of defence is business line management. This means that sound operational risk governance will recognise that business line management is responsible for identifying

and managing the risks inherent in the products, activities, processes and systems for which it is accountable. A functionally independent corporate operational risk function (CORF) is typically the second line of defence, generally complementing the business line's operational risk management activities. The degree of independence of the CORF will differ among banks.

For small banks, independence may be achieved through separation of duties and independent review of processes and functions.

In larger banks, the CORF will have a reporting structure independent of the risk generating business lines and will be responsible for the design, maintenance and ongoing development of the operational risk framework within the bank. This function may include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting. A key function of the CORF is to challenge the business lines' inputs to, and outputs from, the bank's risk management, risk measurement and reporting systems. The CORF should have a sufficient number of personnel skilled in the management of operational risk to effectively address its many responsibilities.

The third line of defence is an independent review and challenge of the bank's operational risk management controls, processes and systems. Those performing these reviews must be competent and appropriately trained and not involved in the development, implementation and operation of the Framework. This review may be done by audit or by staff independent of the process or system under review, but may also involve suitably qualified external parties.

If operational risk governance utilises the three lines of defence model, the structure and activities of the three lines often varies, depending on the bank's portfolio of products, activities, processes and systems; the bank's size; and its risk management approach. A strong risk culture and good communication among the three lines of defence is important characteristics of good operational risk governance.

## 2 INTERNAL AUDIT

Internal audit coverage should be adequate to independently verify that the Framework has been implemented as intended and is functioning effectively. Where audit activities are outsourced, senior management should consider the effectiveness of the underlying arrangements and the suitability of relying on an outsourced audit function as the third line of defence. Internal audit coverage should include opining on the overall appropriateness and adequacy of the Framework and the associated governance processes across the bank. Internal audit should not simply be testing for compliance with board approved policies and procedures, but should also be evaluating whether the Framework meets organisational needs and supervisory expectations. For example, while internal audit should not be setting specific risk appetite or tolerance, it should review the robustness of the process of how these limits are set and why and how they are adjusted in response to changing circumstances.

Because operational risk management is evolving and the business environment is constantly changing, management should ensure that the Framework's policies, processes and systems remain sufficiently robust. Improvements in operational risk management will depend on the degree to which operational risk managers' concerns are considered and the willingness of senior management to act promptly and appropriately on their warnings.

## 3 FUNDAMENTAL PRINCIPLES OF OPERATIONAL RISK MANAGEMENT

**Principle 1**: The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organisation.

**Principle 2**: Banks should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile. Governance the Board of Directors

**Principle 3**: The board of directors should establish, approve and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

**Principle 4**: The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.

**Principle 5**: Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance.

Since the global financial crisis, supervisory approaches are increasingly becoming more direct and more intense to promote the resilience of the financial system. The challenge for supervisors is to strike the right balance between taking a more intensive,

proactive approach and not unduly influencing strategic decisions of the institution's management. Risk culture is an area where a growing number of supervisory authorities are taking a more active role, and the range of supervisory approaches toward assessing risk culture varies. 11 Supervisors are in a unique position to gain insights on risk culture at financial institutions given their access to information and individuals across the institution, as well as the results of supervisory work. This unique view and the ability to gather observations across multiple institutions enable peer analysis and suggest issues that both supervisors and institutions should look at. Supervisors should adopt a process to synthesise periodically supervisory findings, look for common themes, aggregate informal observations they have about the institution and apply high-level judgement in deciding whether culture or undesired behaviour is a root cause of supervisory findings. Supervisors should recognise that every supervisory activity can add information that informs these periodic assessments, but that single supervisory results are rarely a definitive indicator of culture issues that need to be addressed. Evidence should be gathered from the full range of supervisory activities so as to avoid the assessment of risk culture being perceived and managed as a compliance-driven exercise. The lists of possible indicators should be treated as a starting point for those assessments. Supervisors should avoid supervisory methodologies that treat these indicators as a checklist. Which indicator, or indicators, is most relevant to a particular situation will vary. In some cases, underlying factors not specifically mentioned in the detailed indicators will be the source of what the indicators are showing.

Discussions with boards and senior management will help form the supervisory view of the institution's risk culture. Supervisory observations on culture issues should be further discussed with members of the board and senior management so as to promote and develop a shared understanding of the institution's risk culture. Identification of a practice or attitude that is not supportive of sound risk management should be brought to the attention of the board or senior management, as appropriate, who have ultimate responsibility for outlining and overseeing the financial institution's risk culture, to influence change in a positive direction. The supervisor raising, and the financial institution acting early to address, the root causes of the behavioural weakness will aid in preventing (or mitigating the impact of) particular undesired cultural norms from taking root and growing. Supervisors should assess the processes in place by which core values are communicated, understood, embraced and monitored throughout the institution. In particular, supervisors should assess how the board and senior management systematically assess the risk culture of the institution. Supervisors should also assess the extent to which the institution is able to define its risk culture, document the material elements that support it and actively assess gaps and areas of concern to be addressed or enhanced. The institution's willingness to sufficiently document the elements supporting its risk culture should form part of the supervisor's overall assessment. Assessing risk culture is complex and requires a range of skills, tools and approaches. Supervisors need to develop broad-based experience and a set of appropriate skills to derive sensible assessments and interact with institutions at the senior level on the role played by their risk culture. Authorities should ensure that supervisors making these assessments are adequately trained and are able to apply experienced judgement and clearly articulate these judgements. Failure by an institution to remediate findings in relation to risk culture by a supervisor should be subject to the existing suite of supervisory options that is proportional to the size of exposures and materiality of the risks involved. Supervisors should be mindful of unintended consequences in trying to influence risk culture.

***Risk Management Environment Identification and Assessment:***

**Principle 6**: Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood.

**Principle 7**: Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

***Monitoring and Reporting:***

**Principle 8**: Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.

The board and senior management, in their respective roles, set expectations for the risk culture of the institution and may take a range of steps to assess the extent to which those expectations are being met, and address gaps or deficiencies identified. It is critical that the board and senior management demonstrate adherence to sound risk management and the highest standards on integrity (walking the talk), as over time, their behaviour will be emulated by the rest of the institution. Directors with experience in other financial institutions or industries where behaviours and practices generally necessitate a sound risk culture (e.g., healthcare, nuclear energy) can play an important role; non-executive directors are often particularly well placed to bring a fresh perspective and sage advice about issues such as behaviours in relation to overall culture. It is the overarching responsibility of the board and senior management to set the tone at the top, including by clearly articulating the underlying values that support the desired risk culture and behaviours; recognising, promoting and rewarding behaviour that reflects the stated risk culture and its core values; and systematically monitoring and assessing the actual culture. The board and senior management should proactively address behavioural issues and assess

whether they are clearly and effectively articulating and monitoring core values and expected behaviours toward risk. The appropriate tone and standard of behaviour 'from the top' is a necessary condition for promoting a sound risk culture and for ensuring that it is appropriately embedded within the institution. However, it is far from sufficient. For lasting change, the tone and behaviour 'in the middle' is also important to fostering a sound risk culture as it is a channel through which risk culture practices are cascaded further down an institution. Middle-level managers transmit the culture that is derived from leadership to the business lines that have a fundamental role in undertaking risks within the assigned limits of risk exposure and are responsible for identifying, assessing and controlling the risks of their businesses.

***Control and Mitigation:***

**Principle 9**: Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

***Business Resiliency and Continuity:***

**Principle 10**: Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

***Role of Disclosure:***

**Principle 11**: A bank's public disclosures should allow stakeholders to assess its approach to operational risk management.

A vital means of understanding the nature and complexity of operational risk is to have the components of the Framework fully integrated into the overall risk management processes of the bank. The Framework should be appropriately integrated into the risk management processes across all levels of the organisation including those at the group and business line levels, as well as into new business initiatives' products, activities, processes and systems. In addition, results of the bank's operational risk assessment should be incorporated into the overall bank business strategy development processes.

The Framework should be comprehensively and appropriately documented in board of directors approved policies and should include definitions of operational risk and operational loss. Banks that do not adequately describe and classify operational risk and loss exposure may significantly reduce the effectiveness of their Framework. Framework documentation should clearly:

(a) Identify the governance structures used to manage operational risk, including reporting lines and accountabilities.
(b) Describe the risk assessment tools and how they are used.
(c) Describe the banks accepted operational risk appetite and tolerance, as well as thresholds or limits for inherent and residual risk, and approved risk mitigation strategies and instruments.
(d) Describe the bank's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure.
(e) Establish risk reporting and Management Information Systems (MIS).
(f) Provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives.
(g) Provide for appropriate independent review and assessment of operational risk.
(h) Require the policies to be reviewed whenever a material change in the operational risk profile of the bank occurs, and revised as appropriate.

## 4 CONCLUSION

Internal controls are typically embedded in a bank's day-to-day business and are designed to ensure, to the extent possible, that bank activities are efficient and effective, information is reliable, timely and complete and the bank is compliant with applicable laws and regulation. In practice, the two notions are in fact closely related and the distinction between both is less important than achieving the objectives of each. Sound internal governance forms the foundation of an effective operational risk management Framework. Although internal governance issues related to the management of operational risk are not unlike those encountered in the management of credit or market risk operational risk management challenges may differ from those in other risk areas

## REFERENCES


[1] Hedgefund Index (n.d) Market Risk [online] Available at: http://www.hedgefund-index.com/d_marketrisk.asp [Accessed 13 July, 2015]

[2] Kettell, B (2011) Islamic Banking and Finance. UK: John Wiley & Sons Ltd

[3] [3] KPMG (n.d) 'Business Dialogue' [Online] Available at: https://www.kpmg.com/lu/en/services/advisory/risk-consulting/financialregulatoryreporting/documents/operational-risk.pdf [Accessed at 3 Aug, 2015]

[4] [4] Lexicon (n.d) Definition of Risk Management [online] Available at: http://lexicon.ft.com/Term?term=risk-management [Accessed at 3 August, 2015]

[5] [5] Shaikh, S. A & Jalbani, A. A (2009) 'Management in Islamic And Conventional Banks: A Differential Analysis' [online] Available at: http://ssrn.com/abstract=1530393 [Accessed at 15 July, 2015]

[6] [6] Rob D (1992)."Islamic Banking", International Journal of Bank Marketing, Vol. 10 Iss 6 pp. 32 – 37 [Online] Available at: http://dx.doi.org/10.1108/02652329210020321 [Accessed 1 August, 2015]

[7] [7] Tiby, A.M.E (2011) 'Islamic Banking: How to manage risk and increase profitability'. 1st Ed. Canada: John Wiley & Sons Inc.

AUTHORS ADDRESSES

**1** Abdullah Rhoumah Alghwezi

Faculty of Economics, Technical University of Košice, Slovak Republic

E-mail: Abdullah.alghwezi@tuke.sk