# ROLES AND RESPONSIBILITIES FOR MANAGING OPERATIONAL RISK IN A BANKING ENVIRONMENT

*J. Young**

**Abstract**

Operational risk management is one of the fastest growing management disciplines within a banking environment as a result of various disastrous international incidents. Subsequently, various global institutions got involved in order to ensure that the effect of similar events do not negatively influence the international industries, for example, the Basel Committee on Banking Supervision regarding banks. It is, however, a known fact that operational risks are difficult to manage, as it is not easy to quantify. Therefore, it is of the utmost importance to understand the concept of operational risk management and, more specifically, the actual roles and responsibilities of various role-players within an organisation. This paper aims to identify the main role-players involved in the management of operational risk in a banking environment and to identify their specific roles and responsibilities.

**Keywords:** Risk governance, Risk management framework, Risk reporting, Risk control, Risk identification, Risk evaluation

*University of South Africa, PO Box 52 185, Wierda Park, Centurion, Pretoria, South Africa, 0149
Phone: 27 12 429 3725, Mobile: 27 83 307 6265, Fax: 27 12 429 3552
Email: youngj@unisa.ac.za and/or youngj@worldonline.co.za

## 1. Introduction

It is a known fact that operational risk should be regarded and managed as a major risk type by all corporate entities. For example, in the banking industry operational risk is being managed at the same level of importance as credit and market risk. This is proven by the fact that regulators are implementing a regulatory capital allocation for operational risk. However, this is not such a cut and dried approach as it sounds, because there are various requirements to comply with before an organisation can calculate and allocate an accurate and realistic capital charge for operational risk. To ensure an accurate calculation of a capital charge for operational risk, it is imperative to embed a structured approach to manage operational risk. An important issue, in this regard, is to identify and allocate specific roles and responsibilities to various role-players within the organisation to ensure that operational risks are effectively dealt with. Currently there exist some confusion on specific roles and responsibilities regarding operational risk management, which will be addressed to ensure more clarity to some degree. Therefore, the problem statement for this paper is that many role-players involved in operational risk management are not knowledgeable with the detail and extent of their roles and responsibilities. The approach of this paper is to identify the most prominent role-players and the main roles and responsibilities regarding operational risk management. Once the main categories of roles and responsibilities have been identified, a survey will be launched to confirm each role-player's involvement in operational risk management according to respondents from the South African banking sector. A descriptive analysis of the response will be used to confirm the level of involvement for each role-player.

The aim of this paper is to identify specific role-players and their roles and responsibilities to ensure the effective management of operational risk. This could serve as a guideline to organisations when embedding an operational risk management framework and processes. It will, furthermore, ensure that all the role-players at various management levels within the organisation are aware of their contributions to effective risk management and consequent realistic and acceptable capital allocation.

This paper will be divided into the following topics:

- Risk management framework.
- Organisational structure for operational risk management.
- Roles and responsibilities for operational risk management.
- A survey and descriptive analysis of the roles and responsibilities of the main role-players involved in operational risk management in the South African banking industry.

## 2. Operational Risk Management Framework

According to Avarez (2005:227), one of the greatest challenges in today's business environment is the establishment of an enterprise-wide risk management framework that encompasses the many facets of operational risk. Operational risk is not so clear-cut as credit and market risk as it involves all the business activities, whereas credit and market risk specifically relate to business functions. As such, it is necessary for an organisation to develop an ORM framework that covers the entire spectrum of the organisation. According to King (2001:48), an effective framework provides the ability to:

- identify important risks to the firm;
- identify causes for controllable risks;
- classify risk as controllable and uncontrollable;
- assign uncontrollable risks to mitigation categories; and
- provide measurement feedback on changes in risks and relate them to management actions.

However, before an enterprise-wide ORM framework can be developed and implemented, it is important that all the role-players throughout the organisation understand the concept and their specific contributions.

Global operational risk management initiatives confirm the importance of developing and implementing an operational risk management (ORM) framework. The Basel Committee on Banking Supervision, for example, is playing a leading role in establishing and embedding ORM into the banking environment by influencing and guiding the developing of ORM systems and tools. This initiative in finding common ground across the global banking industry is evident of the importance of having an ORM framework in place.

According to a study by Ernst and Young (2005:5), a risk framework should offer a robust foundation of reference for companies interested in implementing risk management. There exist a number of developed frameworks for risk management, which could be used to develop a risk management framework that suits the applicable organisation. A brief sample of the most prominent frameworks is illustrated in table 1.

**Table 1.** Sample of Risk Management Frameworks

| | |
|---|---|
| Australia – New Zealand<br>This standard presents a generic framework for establishing the context and identifying, analysing, evaluating, treating, monitoring and communicating risk.<br>(http://www.standards.co..au) | Committee of Sponsoring Organisations (COSO)<br>Enterprise Risk Management (ERM) – Integrated Framework<br>COSO's Internal Control – Integrated framework has been adopted by many companies in support of their regulatory compliance initiatives<br>(http://www.coso.org) |
| The Federation of European Risk Management Associations (FERMA) Risk Management Standard<br>The Risk Management Standard sets out a strategic process, starting with an organisation's overall objectives and aspirations, through to the identification, evaluation and mitigation of risk, and finally the transfer of some of that risk to an insurer.<br>(http://www.ferma-asso.org) | |

Adapted from Ernst and Young (2005:6)

A common phenomenon amongst these examples is that all refer, to some extent, to the components of a risk management process, which is identified by the Basel Committee (2004:142) as: risk identification, assessment, monitoring and controlling/mitigating. From the aforementioned, the risk management process is evident and can be listed as risk identification, risk measurement, risk control and risk mitigation. King (2001:48), furthermore, states that the objective of operational risk management is to decide which risks are important to the organisation and then to accept, control, or mitigate them in accordance with the risk management strategy of the organisation. However, in order for the risk management process to be effective, it is imperative to establish a clearly defined risk management structure. However, a process on its own is of no use to an organisation without the supporting component of an organisational structure and the governance of the process. As such, it can be deduced that an organisational structure is a second component of a risk management framework.

Although, this research is based on an organisation structure for risk management, as a component of a risk management framework, it is necessary to mention another two components, namely: a risk management culture and a risk management strategy. Young (2006:30) describes these components as follows:

- Strategy – sets the overall tone and approach for operational risk management.
- Culture – refers to the principles and approach of the organisation to manage their risks.

As mentioned above, this research aims to focus on roles and responsibilities of key role-players and will, therefore, focus on the organisational structure for operational risk management.

## 3. Organisational Structure Form

Before embarking on an ORM process, it is necessary to determine who owns the risk. According to Hubner et al (2003:21), risk management must be integrated into the activities of the risk-takers in the organisation. Various regulatory frameworks across countries require a bank to have an independent ORM framework. However, for an independent risk management structure to operate, there has to be an oversight function that operates independently of the risk-takers (risk owners). Once again, if compared with credit and market risk, it is evident that the responsibility of risk-ownership for operational risk is not so clear-cut. An important guideline, however, is that operational risk must be managed as close to the exposure as possible. As such, it is imperative that the employee that is the closest to the exposure should be responsible to manage that risk. However, some operational risks are environmental and are a threat to the organisation as a whole. In these cases it requires the appointment of specific risk managers to take responsibility for the effective management thereof. A typical example in this regard, is an exposure of the organisation to an external threat such as a break in electricity. This could influence the total organisation and requires proactive measures to ensure a continuous flow of business notwithstanding an electricity break. To ensure this, most corporate organisations appointed a business continuity manager. There are various views regarding the optimal structure of an ORM function for corporate organisations such as banks. Although these structures might differ from organisation to organisation, it is imperative to clearly understand the function of ORM and the roles and responsibilities of each role-player.

Many committees and institutions addressed the roles and responsibilities of the various role-players regarding ORM, for example the King Committee on Corporate Governance and the Basel Committee on Banking Supervision. According to the Committee of Sponsoring Organisations of the Treadway Commission (COSO) the responsible parties for risk management include the board of directors, management, chief risk officer, internal auditors and every individual within the organisation.

A typical structure for ORM is illustrated in figure 1.

From this example of a typical structure, focusing specifically on ORM and for the purposes of this paper, the following key role-players can be identified:

- Board of Directors
- Group Risk Management
- Group Executive Committee and CEO
- Internal Audit
- Business Management

Although most institutions describe the roles and responsibilities of the various role-players, there seems to be a lack of practicality when analysing the specific roles and responsibilities. For example, there is often referred to a board of directors that is responsible for assessing risks. When analysing this responsibility in more detail it can be stated that the aim of risk assessments are to determine the risks of the organisation. Risk assessments are usually a bottom-up approach as the risk should be determined as close to the exposure as possible, which is usually at the operating levels of the business. Although the board of directors has a role to play in overseeing the overall policy regarding risk assessments, they will rarely be personally involved in risk assessments at an operating level.

There is various similar examples where responsibilities for risk management are allocated to specific role-players, but when it is analysed, for practical feasibility, it is found to be unpractical and not executable. In this sense, it is important to define the roles and responsibilities of risk management so that each role-player will be able to perform these roles in a way that will add value to the effective management of operational risk. Furthermore, that it is sensible and that all the role-players work together as a unit to ensure the compliance to operational risk management requirements. For the purposes of this research, each of the abovementioned role-player's role and responsibilities toward ORM will be discussed in accordance to various views and requirements. These views and requirements will be analysed to ensure that the roles and responsibilities for each role-player is practical and is allocated to the correct level of responsibility. Based on this analysis a list of roles and responsibilities for each role-player will be formulated to ensure clarity on the total governance of ORM in a corporate banking environment. It is sensible to start with the board of directors, as they are ultimately responsible for the effective management of the organisation's risk and accountable to the shareholders of the company.

## 4. Roles and responsibilities for operational risk management

### 4.1 Board of Directors

Mongiardoino and Geny (2007:43) mention that in the area of risk governance a clear description of the role of the board of directors and its committees in setting the risk appetite for the organisation, overseeing the risk management framework and organisational chart of the risk management function along with a description of the risk communication patterns within the organisation, is required.

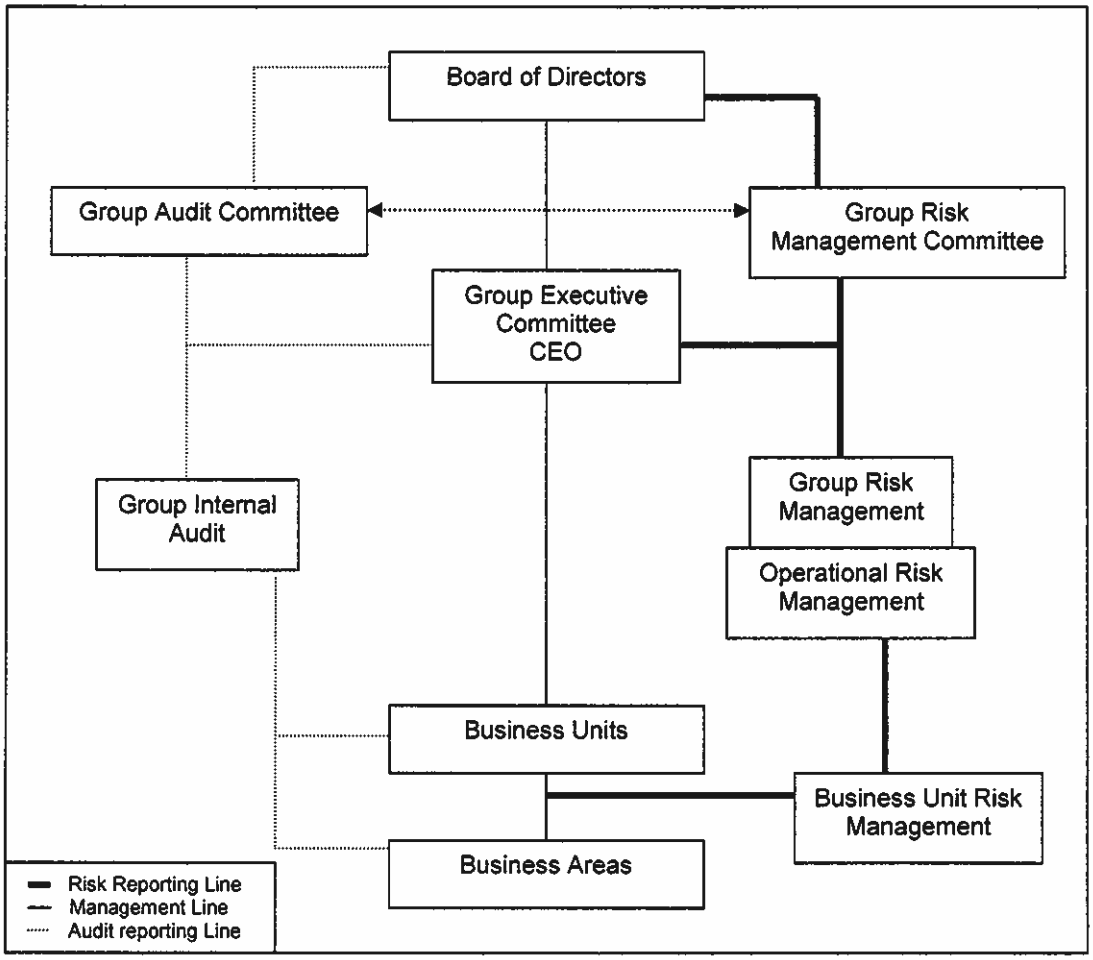


**Figure 1.** A typical Organisational Structure for Operational Risk Management

Effective risk management is one of the main responsibilities of the board and should provide an oversight function with regard to risk management. According to COSO (1992:92), the board should:

- know the extent to which management has established effective risk management in the organisation;
- be aware of and concurring with the organisation's risk appetite;
- review the organisation's portfolio view of risk and considering it against the risk appetite; and
- be apprised of the most significant risks and whether management is responding appropriately.

The board of directors has a major role to fulfill in defining what it expects from senior management at all levels in the organisation regarding risk management. According to Swenson (2003:23), the board of directors and senior management must be actively involved in the oversight of the operational risk management process. The board also plays a role in setting the organisation's strategy, high-level objectives and the corresponding high-level allocation of resources. These factors can be regarded as the basic requirements to enable management to manage the potential risks involved.

The Basel Committee on Banking Supervision (2003:4) has structured a paper on sound practice and principles for risk management. Of these principles also address the role and responsibilities of the board of directors, for example:

- The board of directors should be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed, and it should approve and periodically review the bank's operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored and controlled/mitigated.
- The board of directors should ensure that the bank's operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.

- The board of directors must support the proactive management of operational risk.

Furthermore, every board should have a charter setting out its responsibilities which encompasses:

- adoption of strategic plans;
- effective control and monitoring of operational performance and management;
- determination of policy and procedures to ensure the integrity of the organisation's risk management and internal controls; and
- communications policy and director selection.

In addition, the Basel Committee (2004:141) states that for a bank to qualify to use the Standardised Approach to calculate a capital charge for operational risk, the bank must ensure that its board of directors and senior management are actively involved in the oversight of the operational risk management framework.

The organisation's board should define and document its policy for managing risk, including the objectives for and its commitment to risk management. The policy may include the following:

- The objectives and rationale for managing risk.
- The links between the policy and the organisation's strategic plans.
- The extent and types of risk the organisation will take and the ways it will balance threats and opportunities.
- The processes to be used to manage risk.
- Accountabilities for managing particular risks.
- A statement on how risk management performance will be measured and reported.
- Details of the support and expertise available to assist those accountable for managing risks.
- A commitment to the periodic review of the risk management system.
- A statement of commitment to the policy by directors and the organisation's executives (ANZ Standards 2004:27).

It is important to establish accountability and authority for risk management. The directors and senior executives are ultimately responsible for managing risk in the organisation, although, all staff is responsible for managing risks in their areas of control. This may be facilitated by:

- specifying those accountable for the management of particular risks or categories of risk, for implementing treatment strategies and for the maintenance of risk controls;
- establishing performance measurement and reporting processes; and
- ensuring appropriate levels of recognition, reward, approval and sanction (ANZ Standards 2004:27).

According to the Basel Committee (2004:159), a sound risk management process is the foundation for an effective assessment of the adequacy of a bank's capital position. Bank management is responsible for understanding the nature and level of risk being taken by the bank and how this risk relates to adequate capital levels. As such, the board and senior management should thus view capital planning as a crucial element in being able to achieve its desired strategic objectives and to achieve this has the following responsibilities:

- to set the bank's tolerance for risks;
- to ensure that management establishes a framework for assessing the various risks;
- to develop a system to relate risks to the bank's capital level;
- to establish a method for compliance with internal policies;
- to adopt and support strong internal controls and written policies and procedures; and
- to ensure that management effectively communicate these policies and procedures throughout the organisation.

In addition, banks should have a formal disclosure policy approved by the board of directors that addresses the bank's approach for determining what disclosures it will make and the internal controls over the disclosure process (Basel 2004:177).

A previous King Report (King I) dated 1994, spells out 15 important principles of corporate governance for boards of directors and persons responsible for the direction of a business enterprise. Of these principles, the following mention the role of the board and state that the board should:

- determine the corporation's purpose and values, determine the strategy to achieve its purpose and to implement its values in order to ensure that it survives and thrives and ensure that procedures and practices are in place that protect the corporation's assets and reputation;
- monitor and evaluate the implementation of strategies, policies, management performance criteria and business plans;
- ensure that the corporation complies with all relevant laws, regulations and codes of best business practice;
- ensure that the corporation communicates with shareholders and other stakeholders effectively;
- identify the corporation's internal and external stakeholders and agree on policy, or policies, determining how the corporation should relate to them;
- ensure that all technology and systems used in the corporation are adequate to properly run the business and for it to remain a meaningful competitor; and
- identify key risk areas and key performance indicators of the business enterprise and monitor the factors (Valsamakis et al 2004:74).

It is recognised that for practical purposes, it is sometimes necessary for a board to delegate certain of its responsibilities and functions to one or more

committees to carry out the identified overseeing responsibilities regarding risk management.

According to Ernst and Young (2005:12), to promote an active dialogue between executive management levels and a consistent approach to risk assessments, organisations should form a risk committee. This committee should meet often enough to ensure that key risk issues could be communicated and discussed on a timely basis.

Analysing the abovementioned roles and responsibilities of the board of directors of a bank, their main roles and responsibilities regarding risk management can be categorised as follows:

- Governance
  - Approval of a risk management framework.
  - Approval of risk policies and standards.
- Strategic planning
  - Consider main risks during strategic planning.
  - Approval of the risk appetite.
  - Capital allocation for risks.
- Risk control
  - Making of strategic business decisions.
- Reporting
  - Disclosures to shareholders.
  - Ensuring regulatory compliance.

A group risk management function also plays an important role and will be discussed next.

## 4.2 Group Risk Management

According to Swenson (2003:22), risk managers are aligned alongside line managers and, at this level, usually perform an administrative role in terms of coordinating specific enterprise-wide risk management functions, whereas the line management is responsible to take the ownership of the actual risk management process. Swenson (2003:23) states that a centralised risk management function is responsible for setting risk management policies and facilitating development of operational risk reporting. In addition the group risk management is usually responsible and accountable for enterprise-wide risk management, which includes the establishment of enterprise-wide key risk indicators to ensure a standardised risk and control environment. As such, it is imperative that a group risk management team must ensure standardised risk management methodologies and mechanisms. This will allow the organisation to use a standardised reporting approach, which will ensure that the board of directors and senior management use the same information to base their business decisions on.

A group structure should include specialists in risk management and should therefore be the center of a bank's knowledge on risk management. As such, a group risk function should ensure a continuous research and development ability that would provide knowledge on leading and best practices regarding risk management. Furthermore, the group risk function should be the hub for risk management training for all involved role-players to be able to perform their risk management functions.

Another primary responsibility of a group risk management function is to coordinate all risk management information on a centralised basis. This would ensure a central repository for risk information that is accessible by all the role-players.

In conclusion, the roles and responsibilities of a group risk management function could be summarised as follows:

- Governance
  - Coordinating risk management policies and standards on behalf of the board of directors.
  - Research and development of risk management practices.
  - Coordinate risk management training.
- Strategic planning
  - Provide risk-related information and expertise during strategic planning processes.
  - Coordinate all risk information as a basis to determine the overall risk profile and the risk appetite.
- Risk control
  - Monitoring the implementation of risk policies and standards.
  - Monitoring the use of risk management practices.
- Reporting
  - Consolidate risk reports to the board of directors/risk committees.
  - Consolidate all risk information on a centralised basis on behalf of the organisation.
  - Coordinate the risk reports to various stakeholders such as the regulator.

The next important role-player(s) is the group executive committee, which includes the CEO.

## 4.3 Group Executive Committee and CEO

Group executive committees and the CEO can be regarded as senior management and are more closely involved in the function of risk management than the board of directors. However, in order to perform this role effectively, it should be made clear what exactly is expected from senior management. According to the Basel Committee (2004:141), the board of directors and senior management must be actively involved in the oversight of the operational risk management framework. The main question in this regard is how can banks achieve and ensure this requirement in terms of the actual functions of senior management relating to risk management?

Ernst and Young (2005:7) states that directors and executives share a common desire and that is to benefit from a risk summary report that describes key risks, how they are managed and monitored, key issues and accountability. A key risk summary report can assist directors to understand the key risks facing the organisation and can use this report to track and oversee the status of key risks. This will allow line

management to better prioritise and report the status of key risks and related activities. It can also assist line management to focus on the key roles and related activities.

According to ANZ standards (2004:26), the support of senior management is important for effective risk management and their awareness and commitment may be achieved by the following:

- Obtaining the active and ongoing support of the organisations directors and senior executives for risk management and for the development and implementation of the risk management policy and plan.
- Appointing a senior manager to lead and sponsor risk management initiatives.
- Obtaining the commitment and support of all senior managers for the execution of the risk management plan.

The CEO's (in cooperation with senior executive management) responsibilities include ensuring that all components of risk management are in place. This duty generally includes the following:

- Setting the organisation's strategy and formulate the overall objectives.
- Providing leadership and direction to senior managers.
- Setting broad-based policies and develop the organisation's risk appetite and culture.
- Take actions and make decisions concerning the businesses' risks and ensure communication of key policies and the reporting processes that will be used.
- Record details of risks, controls and priorities.
- Manage risk incidents and loss events and the lessons learned.
- Take and allocate accountability for risks, controls and treatments.
- Track progress of risk mitigation actions.
- Monitor progress against the risk management strategy.

In conclusion the main responsibilities of executive management and the CEO can be summarised as follows:

- Governance
  - o Approval of business-specific policies and procedures for risk management within the framework of overall risk policies and standards approved by the board of directors.
  - o Appointment of risk managers and risk owners.
  - o Overseeing the implementation of the approved risk management framework.
- Strategic planning
  - o Setting the overall strategy and objectives for the business.
  - o Setting the risk appetite for the business.
- Risk control
  - o Obtaining commitment and support of senior management for the execution of risk management plans.
  - o Take action and make decisions concerning the effective management of risks.
  - o Monitor the execution of risk action plans.
  - o Record details of risks, controls and priorities (risk register).
- Risk reporting
  - o Report key risks to the board of directors.
  - o Evaluate risk reports and communicate decisions where applicable.

The next important role-player in risk management is internal audit.

## 4.4 Internal Audit

Traditionally, internal audit has served as the first line of defence against operational risks and focused on the weaknesses in internal controls. As such, internal audit was originally responsible for operational risk management, although they concentrated more on the operations, including systems and processes, rather than operational risk *per se*. However, since operational risk was more clearly defined as the risk of loss due to inadequate or failed internal processes, systems and people or from external events, it became necessary to develop a more focused management approach. Hence, it required that internal audit's role towards risk management had to change from risk management to independent internal auditor.

According to Ernst and Young (2005:13) the internal audit function is one of the board's most powerful mechanisms for understanding the full spectrum of the key risks facing the organisation and monitoring the effectiveness of related controls and risk management processes. As such, it is important that there should be a close relationship between the Board Audit Committee and the Board Risk Committee.

Furthermore, with the recent developments in the management of operational risk in terms of the Basel requirements, operational risk management became a specialised management discipline. This requires that the functions of risk management must be specifically addressed during a formal risk management strategy, rather than an additional task for internal audit. As soon as an organisation realises the extent of this management function and allocate it to a separate risk management structure to manage, it becomes imperative that internal audit functions independently. This will ensure that the effectiveness of risk management can be objectively audited by internal audit to provide top management with the assurance that risks are being managed properly.

The internal audit function needs to ensure and provide assurance that the operational risk management process has integrity and is being implemented along with the appropriate controls. Internal audit should also offer an independent assessment of the underlying design of the operational risk management process. This includes examining the processes surrounding the building of operational risk management models; the adequacy and reliability

of the operational risk management systems and processes; and compliance with external regulatory guidelines. Internal audit thus provides an overall assurance on the adequacy of operational risk management. This should also include the examination of controls concerning the capturing of data. Internal audit would typically also review the adequacy and effectiveness of the processes for monitoring risk management processes.

Risk reporting forms another important part of an internal audit function. However, risk reports which can enhance future growth opportunities, representing those strategies and supporting objectives which an organisation is pursuing could potentially increase competitive advantage, is often overlooked as internal audit tends to focus more specifically on risk assessment reports which focus on risk controls at a business process level.

The role of internal audit relating to risk management can be summarised as follows:

- Governance
  - Provide top management with the assurance that risks are being managed according to the approved policy and standards and within the approved risk management framework.
- Strategic planning
  - Ensure that all risks are addressed during the strategic planning process.
  - Provide input during a realistic setting of the risk appetite based on audit reports.
- Risk control
  - Monitor the effectiveness of risk management practices.
  - Monitor the effectiveness of risk management controls (internal controls).
  - Monitor the adequacy of risk management systems and processes.
- Risk reporting
  - Audit reports on the efficacy of risk management provide a powerful mechanism to management to ensure an effective risk management framework.

The final important role-player in risk management is the business manager (business management).

### 4.5 Business Management

Business management is regarded as the line function to ensure the future growth and existence of the organisation. Business management has a primary obligation to report to the board of directors as well as the shareholders of the organisation. As such, it is imperative to report on the shareholder value in terms of the current and future strategies and objectives of the organisation as well as the main processes that support the strategies and objectives. It is, furthermore, imperative to also consider the risks involved. This concept can be illustrated by means of a diagram (refer to figure 2).

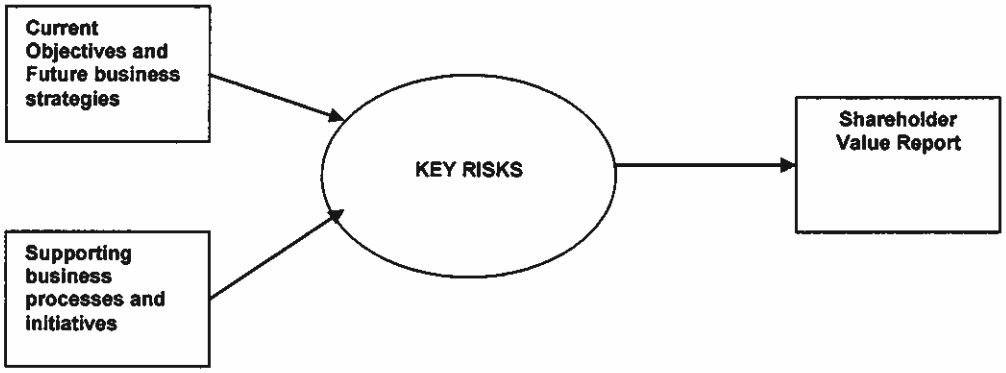


**Figure 2.** Report on Shareholder Value

According to Ernst and Young (2005:8), it is also important to consider the processes that are inherently risky, but do not directly generate significant profits, especially those that involves a substantial portion of capital at risk.

From a risk management perspective, risk identification and evaluation forms the first important activity of business management. Risk assessment is an important risk management function that must be performed from a bottom-up approach. It often happens that this function is performed at an ad hoc basis or once-off basis. In order to ensure a continuous risk assessment process, risk assessments should be evolved into a consistent, embedded activity within the organisation's strategic, business, budget and audit planning processes, rather than executed as a significant stand-alone process. In order to achieve this objective, it is important to appoint a dedicated risk coordinator and a common risk reporting method, which could be regarded as an important function at a business management level.

Current and future business growth opportunities and supporting activities are the primary source of risk reports as it usually includes planning documents such as strategies, business objectives, budgets, business processes and products and internal audit reports and findings. These are valuable documents to use during a risk and control self-assessment process,

which will determine the most significant risks to achieving the objectives and business initiatives.

Data aggregation forms another important part of risk management. As such, it is required that the businesses are responsible to aggregate their risk data in order to make business decisions. There are various risk management methods to assist risk management, for example:

- Risk and control self-assessments.
- Loss history.
- Key risk indicators.
- Scenarios.
- Process flow analysis.

The use of these methods should be developed and implemented by businesses. This will allow businesses with the capability to determine risks at the lowest level of exposure and to identify control measures to prevent or minimise the effects of a risk event. Furthermore, it allows operating managers to determine and monitor action plans to control and manage the identified risks. Business management could be regarded as the execution level of risk management, receiving their mandate from the board of directors and senior management. As such, business management is the risk owners as far as their specific business activities are concerned. Consequently, it requires that business management is primarily responsible to identify all the risks for their business activities and implement adequate control measures for these risks.

Risk managers are often appointed by business management to assist in the management of the businesses' risks. The roles and responsibilities of these risk managers can be deduced from the roles and responsibilities of the group risk management function, but at a business unit level.

The roles and responsibilities of business management can be summarised as follows:

- Governance
  - Appoint specific accountable risk owners as close to the risk exposures as possible.
  - Ensure the execution and implementation of risk management policies by developing detailed risk management procedures.
- Strategic planning
  - Ensure the execution of the risk management process during the strategic planning process. This includes, risk identification and evaluation (measurement and assessment).
- Risk control
  - Implement internal control measures to address identified risks.
  - Continuous monitoring of control measures.
  - Ensure the controlling of risks at the point of risk exposure.
  - Implement an incident management system to monitor and address risk incidents/events that could incur losses.
- Risk reporting
  - Implement a bottom-up risk reporting process to ensure that all risks are addressed.
  - Manage key risk indicators to monitor current risks that could negatively influence the successful achievement of business objectives.
  - Ensure a reporting process to communicate risks to the executive management and board of directors that could affect the total organisation.

## 5. Conclusion

Risk management is initiated by a number of role-players, each with important responsibilities and contributions. The board of directors (sometimes through risk committees), risk managers, internal auditors and business managers are crucial role-players to ensure an effective risk management process throughout the organisation. In actual fact everyone in the organisation has to some degree a responsibility for risk management.

The risk management roles and responsibilities can be divided into the following main categories and activities:

- Governance. This activity entails the overall management of an organisation that includes the responsibilities of ensuring the effective management of risks that the organisation faces.
  - Risk management oversight. This involves an overall control and monitoring function to ensure the effective management of risks throughout the organisation.
  - Authorising/approving the ORM framework. A risk management framework includes the total approach of an organisation to risk management, which includes the following:
- Risk management strategy
- Risk structures including committees
- Risk management culture
- Risk management processes
  - Risk management policies and standards. From a governance perspective, it is imperative that risk policies and standards be approved at the highest level to provide the accountable staff with the mandate to assume the respective roles and responsibilities for risk management.
  - Regulatory compliance. It is important that regulatory compliance be monitored at a corporate level, as this is a regulation of the overall state of risk management in the organisation. As such, the board of directors is

responsible for the regulatory reports and consequent results.

- Risk management methods. To ensure effective corporate governance from a risk management perspective, it is imperative to develop standardised risk management methods. This would ensure a standardised and structured approach to risk management and reporting methods, which will ensure a uniform input from various business units to establish an overall risk profile for the organisation.
- Risk appetite. A risk appetite should be part of the corporate governance of an organisation, as the board of directors must approve it. The risk appetite confirms the overall risks of the organisation and how the organisation will be managing these risks.
- Capital allocation. Allocating capital for potential major disastrous risk incidents.
- Risk management training. To ensure that all the role-players are adequately trained in terms of their roles regarding risk management.

- Strategic planning. This entails the setting of the overall business strategy and objectives of the business. During this process it is imperative that risks be identified, evaluated and addressed in a suitable way to ensure the optimum achievement of business objectives. As such, it is clear that the following components of the risk management process play an integral role during strategic planning:
  - Risk identification and evaluation. Risk identification and evaluation involves the more active part of operational risk management and should be executed at an operating level to determine the risks and evaluate it to formulate management plans. Various tools are available to assist in risk identification and evaluation, for example:
    - Risk and control self-assessments.
    - Risk incident management.
    - Process flow analysis.
  - Setting of realistic risk appetite.
- Risk control. Risk control aims to address the identified risks in terms of control measures and involves the participation at various management levels. It is, however, important to control the identified risks as close to the exposure as possible. During the process of risk control, the objective is to address the exposures in terms of accepting the risk as part of normal business procedures, implementing control measures, transferring the effect of a potential risk event to a third party (insurance), or allocating capital for a potential risk. In order to control the risks, the main activities, identified, are as follows:
  - Making strategic risk control decisions.
  - Monitoring the implementation of risk policies and standards.
  - Monitoring the adequacy of risk management systems and processes.
  - Ensuring effective controls of risks as close to the risk exposure as possible.
  - Risk monitoring process. The aim of monitoring the risk management process on a continuous basis is to ensure that all risks are identified, evaluated, reported and controlled.
- Risk reporting. Risk reporting is probably one of the most important components of a risk management process. It involved the bottom-up reporting of identified risks and a top-down communication of decisions on actions to mitigate the risks. As such, the main activities are as follows:
  - Disclosures of risks and risk management to stakeholders.
  - Reporting on regulatory compliance regarding risk management.
  - Bottom-up risk reports and communication.
  - Top-down risk decisions and communication.
  - Audit reports of the efficacy of risk management processes and systems.

The levels of involvement in risk management can be divided into the following categories (refer to figure 3):

- Oversight. This involves management at an approval level that approves the way risks must be managed within the organisation.
- Decision-making. This involves the making of important business decisions that will also address the identified risks.
- Support. This entails the element of business support, which will ensure the effective risk management decisions.
- Execution/control. This includes the active management of risks by means of implementing the approved control measures.

## 8. Survey

To confirm the abovementioned discussion on the roles and responsibilities of specific role-players in the management of operational risk in the South African banking environment, a survey was launched to confirm the roles and responsibilities and the level of involvement of the identified role-players regarding operational risk management in a banking environment

The survey was conducted by means of a closed questionnaire that was divided into primary risk management activities, namely: governance, strategic planning, risk control and risk reporting. Detailed risk management functions were allocated to each activity according to the research in this paper. Respondents had to identify the level of involvement for each role-player in terms of the following:

- Oversight
- Decision-making

- Support
- Control

The graph in figure 4, confirms the level of involvement of each role-player. According to the response, it is clear that the board of directors has an overwhelming oversight role (80.2%); group risk management mostly a supporting role (48%); the CEO and executive committee a dual role of decision-making (31.8%) and oversight (32.4%); business management a control function (71.2%); and internal audit a supporting role (42.7%).

Furthermore, and according to an analysis of the survey, the main role and responsibilities of the main role-players can be illustrated in table 1.

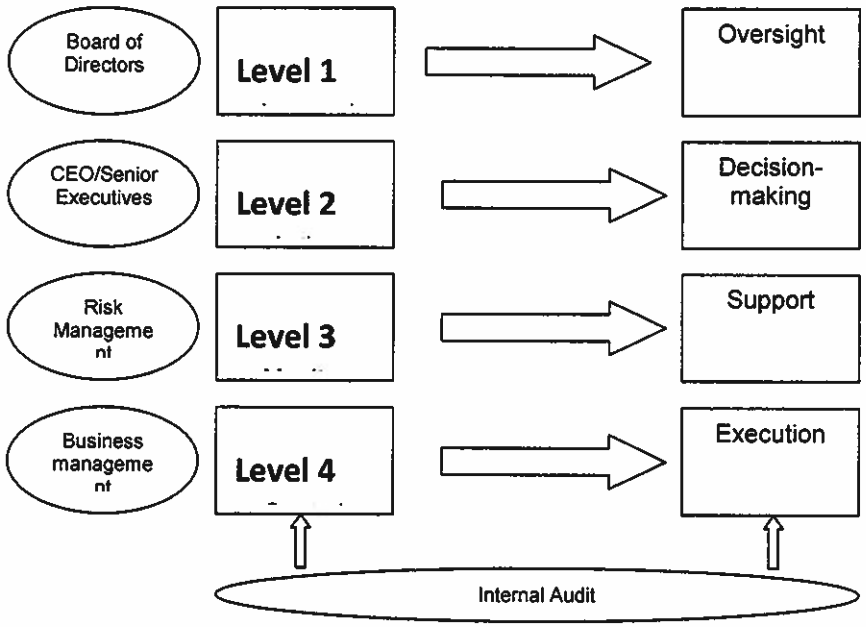


**Figure 3.** Levels of Involvement in Risk Management

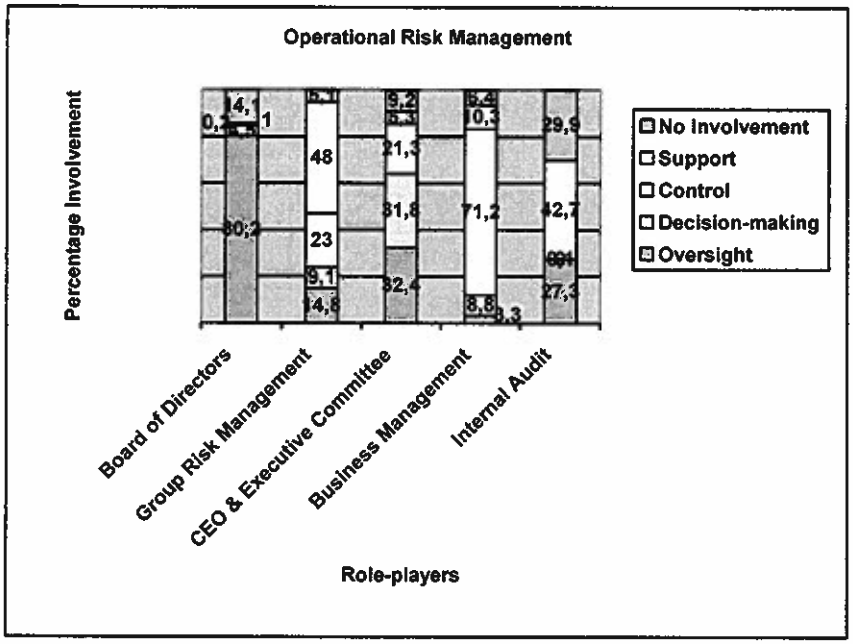


**Figure 4.** Percentage involvement of the role-players in operational risk management for each involvement category

Results of a survey dated July 2007

**Table 1.** The level of involvement of the role-players for each category of responsibility

| Role-players | Governance | Strategic planning | Risk control | Risk reporting |
|---|---|---|---|---|
| Board of directors | Oversight | Oversight | Oversight | Oversight |
| Group risk management | Support | Support | Oversight | Control |
| CEO and senior executives | Oversight | Decision-making | Oversight | Decision-making |
| Business management | Control | Decision-making | Control | Control |
| Internal audit | Support | Support | Oversight | Support |

According to the response, it can be concluded that the board of directors has an oversight responsibility towards all the main risk management categories. Group risk management has a supporting responsibility for governance and strategic planning, an oversight responsibility for risk control and a controlling responsibility for risk reporting. The CEO and executive management has a dual responsibility in terms of oversight for governance and risk control and a decision-making responsibility for strategic planning and risk reporting. Business management has a control responsibility for all the categories except a decision-making responsibility for strategic planning. Internal audit has a supporting responsibility towards governance, strategic planning and risk reporting and an oversight responsibility for risk control.

The response indicates that the board of directors has an overall oversight role in terms of risk management. The following functions were indicated as the most important:

- Approval of an operational risk management framework (Governance).
- Approval of a risk appetite (Governance).
- Approval of a risk capital allocation for operational risk (Strategic Planning).

The respondents identified the main functions under each level of involvement for a group risk management department as follows:

- Support
  - Approval of operational risk management methodologies (Governance).
  - Approval of the operational risk appetite (Strategic Planning).
  - Approval of capital allocation for operational risk (Strategic Planning).
- Oversight
  - Embedding an operational risk management culture for the organisation (Governance).
  - Implementing operational risk management methodologies (Control).
  - Monitoring the implementation of operational risk management policies and standards (Control).
- Control
  - Coordinating operational risk management reports for the bank (Reporting).
  - Compiling operational risk management reports to external stakeholders (reporting).
  - Providing operational risk management training (Control).

The respondents indicated the following most important functions under each level of of involvement for the CEO and executive management:

- Oversight
  - Developing an operational risk management framework (Governance).
  - Strategic planning for business units (Strategic Planning).
  - Making strategic operational risk management decisions (Strategic Planning).
  - Monitoring the efficacy of operational risk management policies and standards (Control).
  - Operational risk management reporting (Reporting).
  - Monitoring key risk indicators (Control).
- Decision-making
  - Approving the operational risk management framework (Governance).
  - Embedding an overall operational risk management culture (Governance).
  - Ensuring a formal operational risk management structure (Governance).
  - Allocating responsibility for operational risk management (Governance).
  - Setting operational risk management strategy (Strategic Planning).
  - Approval of risk appetite (Strategic Planning)
  - Transferring of potential effects of operational risk – insurance (Control).
  - Strategic operational risk management decisions (Strategic Planning).

Business management was mainly categorised at a control level of risk management that included the following main risk functions:

- Control
  - Ensuring the effective management of operational risks (Governance).
  - Approving of formal operational risk management processes (Governance).
  - Approving operational risk management policies and standards (Governance).
  - Ensuring regulatory compliance regarding operational risk management (Control).

- Implementing operational risk management methodologies (Control).
- Implementing operational risk management strategy (Control).
- Compiling operational risk appetite (Control).
- Providing operational risk management training (Control).
- Controlling operational risk exposures (Control).
- Developing and implementing internal controls for operational risks (Control).
- Managing the operational risk profile (Governance).
- Compiling operational risk reports (Reporting).

▪ Decision-making

- Implementing operational risk policies and standards (Control).
- Approval of operational risk management methodologies (Control).
- Strategic planning for the business (Strategic Planning).
- Transferring the potential effects of operational risks – insurance (Control).

The respondents rated internal audit mainly as a supporting role-player which includes the following main risk management functions for each level of involvement:

▪ Support

- Ensuring the effective management of operational risk (Governance).
- Developing an operational risk management framework (Governance).
- Implementing operational risk management policies and standards (Control).
- Strategic planning for the business (Strategic Planning).
- Coordinating of operational risk management reports (reporting).
- Compiling operational risk management reports (Reporting).
- Developing and implementing internal controls for operational risk (Control).

It is evident that the results of the survey confirms and emphasises the various roles and responsibilities, which was identified during this research. As such, it is envisaged that this paper could serve as a solid platform for organisations when developing and implementing an operational risk management function and that it will assist in ensuring that the primary role-players in risk management is more knowledgeable in terms of their involvement in the risk management process.

## References


1. Alvarez, G. (2005). *Operational Risk: Practical Approaches to Implementation*. Edited by E. Davis. London: Risk Books.
2. Australia/New Zealand Standards Committee (AZN). (2004). *Risk Management*. AS/NZS 4360:2004. Third edition 31 August 2004.
3. Basel Committee on Banking Supervision. (2003). *Sound Practices for the Management and Supervision of Operational Risk*. Bank for International Settlements.
4. Basel Committee on Banking Supervision. (2004). International Convergence of Capital Measurement and Capital Standards. Bank for International Settlements.
5. Committee of Sponsoring Organizations (COSO) of the Treadway Commission. (1992). Internal Control-Integrated Framework. Jersey City: American Institute of certified Public Accountants.
6. Ernst & Young, (2005). Managing Risk Across the Enterprise – Connecting New Challenges with Opportunities. *Emerging trends in Internal Controls* – Fourth Survey, Ernst & Young, September 2005.
7. Hubner, R. laycock, M and Peemoller, F. (2003). *Advances in Operational Risk: Firm-wide Issues for Financial Institutions*. Edited by SAS. London: Riskbooks.
8. King Committee and Commission on Corporate Governance. (2002). *King 2 Report on Corporate Governance for South Africa. Draft for Public Comment*. Pretoria: Institute of Directors in Southern Africa.
9. King, J.L. 2001. Operational risk: measurement and Modelling. West Sussex, John Wiley & Sons, Ltd.
10. Mongiardino, A. and Geny, H. (2007). Financial Services: The Need for More Robust and Transparent Disclosures. *GARP Risk Review*. A Publications of the Global Association of Risk Professionals. January/February 2007:38-43.
11. Swenson, K. (2003). A qualitative operational risk framework: guidance, structure and reporting. Edited by Carol Alexander. London. Pearson Education, Ltd.
12. Valsamakis, A.C., Vivian, R.W., & Du Toit, G.S. (2000). *Risk Management: managing enterprise risks*. 3rd edition. Johannesburg: Heinemann.
13. Young, J. (2006). Operational Risk Management: The practical application of a qualitative approach. Pretoria Van Schaik Publishers.