GUIDING CRITERIA FOR OPERATIONAL RISK REPORTING IN A CORPORATE ENVIRONMENT

*J. Young**

Abstract

Risk reporting is most probably one of the most important components of a risk management process. Operational risk reporting, in many organisations, is not developed to such a degree that it will add value to the organisation and is mostly based on regulatory requirements. This means that risk reports mostly aim to comply with regulations rather than add value in terms of providing useful information to ensure effective decision-making. Within this context, this research aims to develop guidelines for operational risk reporting which will be based on a comprehensive literature review of operational risk to determine criteria which can serve as guidelines for effective risk reporting. The criteria will be subject to an empirical analysis by means of an anonymous questionnaire completed by experienced managers in a corporate environment. The data will be analysed in terms of descriptive statistical analysis in order to confirm the applicability of the criteria in terms of operational risk reporting. The information will be used to compile a prioritised list of criteria which could serve as a guideline to corporate organisations during operational risk reporting.

Keywords: Integrated Risk Reporting, Risk Reporting, Risk Control, Risk Communication, Operational Risk Management, Key Risk Indicators, Risk Incidents, Risk Identification, Risk Assessment, Risk Information, Residual Risk, Inherent Risk, Risk Owner

**University of South Africa, PO Box 52185, Wierda Park, Centurion, Pretoria, South Africa, 0149*
Tel: +27 12 429 3010, +27 8307 6265

1 Introduction

The management of operational risk, as an independent risk type and management discipline should be in an advanced phase of implementation in most organisations. There are a number of reasons to support this statement, seeing that the management of operational risk started in earnest in the 1990's and should, therefore, after twenty-five years be recognised as a reasonably matured risk management discipline in its own right. It seems that most organisations accepted the Basel Committee on Banking Supervision's (BCBS) definition of operational risk as the risk of losses due to inadequate or failed internal processes, systems, or people, or because of external events. This definition also includes legal risk, but excludes reputational and strategic risks. (BCBS, 2003). Since the Basel Committee on Banking Supervision (2006) promulgated the regulatory framework for the banking industry, providing guidelines to link a minimum capital to risks, most organisations focused on the embedding of a structured approach to risk management. This is also true for operational risk management in the sense that banks, for example, must also allocate a capital charge for this risk type. In this regard, the BCBS (2006) reiterated that a bank should develop a framework for managing operational risk and evaluate the adequacy of capital. According to Gregoriou (2009), the framework on Capital Measurement and Capital Standards for the banking sector has now gone live in most parts of the world and includes the covering of operational risk. It is therefore, imperative that banks and all other corporate organisations should have an operational risk management framework to ensure that the approach to operational risk management is sound and structured. A risk management framework is described by the Australian/New Zeeland Standard (AS/NZS) (2004) as a set of elements of an organisation's management system concerned with managing risk. Young (2014) mentions that the aims of an operational risk management framework are to identify and establish a structured approach to the management of operational risk and to serve as a guideline on how to achieve the following goals: the establishment of an integrated risk management environment; development of cultural awareness of risk management; development of roles and responsibilities relating to risk management; and providing a common understanding of operational risk. Girling (2013) states that a strong risk framework provides transparency into risks in the firm, therefore allowing for informed business decision-making. In addition, Girling (2013) mentions that with such a strong operational risk management framework a firm can avoid bad surprises and equip itself with tools and contingency planning to be able to respond swiftly when an event does occur. An important part of a risk management framework is a formalised and embedded risk management process. According to Chapman (2011), to implement a risk framework activity within the overall risk management framework includes the implementation of the risk management process. As such, it can be deduced that an organisation should ensure that it has an embedded risk management framework, which by implication also means an effective risk management process. According to the International Organisation for Standardisation (ISO 31000) (2009), it is recommended that organisations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organisation's overall governance; strategy and planning; management; reporting processes; policies; values; and culture.

In view of the aftermath of the financial crisis, a concept that is currently under scrutiny is the concept of integrated reporting. According to Makiwane and Padia (2012), integrated reporting is a new concept not only in South Africa but all over the world. In the King Report on Governance for South Africa (King III) (2009), it is defined as an integrated representation of the company's performance in terms of both its finances and its sustainability. According to Verschoor (2014), integrated reporting focused on the combining of financial reporting with responsibility reporting concerning social issues, governance and the environment. Integrated reporting can be regarded as the integration of the annual financial report with various sustainability reports. Eccles, Krzus and Tapscott (2010) define integrated reporting as the process of environment, social and governance integration into the annual report. According to James (2014), a trend towards combining sustainability and financial reporting is emerging and referred to as integrated reporting. It seems that although most organisations are conforming to the concept of integrated reporting, the concept is still new (and sometimes vague) and to establish an integrated reporting process, it should be clear what must be included in such a process and subsequent report. Risk reporting forms an integral part of sustainability reporting, but it sometimes seems that organisations perform risk reporting without a clear objective in mind. It is imperative that risk reporting (including operational risk reporting) should be managed by reporting criteria in order to ensure that reports are adequate and will add value as part of an integrated reporting process. Therefore, the research question applicable to this research is: are there clear guideline criteria for operational risk reporting as an input to an integrated reporting process?

In order to address the research question, the focus of this article is on operational risk reporting which can be regarded as an essential component of a risk management process. Therefore the purpose of this article is to provide guiding criteria for effective operational risk reporting which could add value to a proactive approach to manage operational risks and to serve as a valuable input for integrated reporting. Various views on risk reporting will be analysed in order to identify guiding criteria for organisations to ensure effective and timely operational risk reports.

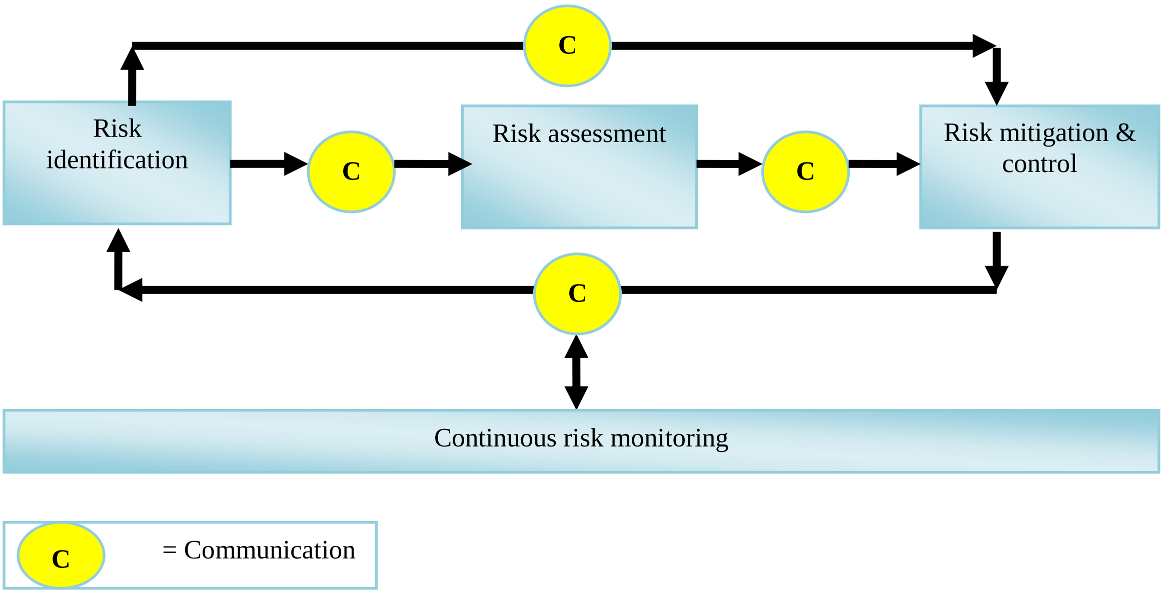
According to King (2014), "reporting has become far more complex since the days when financials were the only area on which organisations needed to report. This has led to increased pressure for a model that enables reporting across a broad spectrum of functions". In this sense and in terms of the purpose of this paper, the concept of risk reporting will be emphasised as an integrated part of a risk management process. As such, to identify, the criteria for operational risk reporting, it is necessary to deal with the operational risk management process as the underlying concept for effective risk reporting.

2 Operational risk management process

ISO 31000 (2009) infers that the risk management framework assists in managing risks effectively through the application of the risk management process. Therefore the framework should ensure that information about risks is derived from the risk management process and it should be adequately reported and used as a basis for decision-making and accountability at all relevant management levels.

Many authors and institutions identified different, but mostly similar, components of an operational risk management process. For example, the AS/NLS standard (2004), indicates that risk management involves the establishing of and applying a logical and systematic method of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risks. The ISO 31000 (2009) indicates that a risk management process is a systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk. According to Young (2014:46), the operational risk management process can be defined as the systematic application of risk policies, procedures and practices by means of the identification, evaluation, control, financing and monitoring of operational risks. Girling (2013:219) mentions that an operational risk framework is designed to identify, assess, monitor, control and mitigate operational risk. It is clear that there is mostly a common understanding of the components of a risk management process. However, according to Chapman (2008:11), a way of exploring the mechanisms for implementing a risk management process is to break it down into its component parts and examine what each part should contribute to the whole. As such he (2008:11) proposes that the risk management process be broken down into six components, namely analysis, identification, assessment, evaluation, planning and management. It is however apparent that from most of the aforementioned views, it seems that communication is a crucial part of an operational risk management process and without this component such a process will not be able to function. As such, communication can be regarded as a common component ensuring the success of a risk management process. Based on some of the mentioned components of a typical risk management process, it can be illustrated as set out in figure 1.

Figure 1. Components of an operational risk management process



It is clear that communication creates a link between all the components of a typical operational risk management process. Firstly, it is important that there is a clear communication process between risk identification and risk assessment in order to ensure that the identified risk exposures can be assessed and evaluated to determine the residual risks that must be mitigated and controlled. Secondly, once the residual risks are determined, it must be mitigated in order to prevent the risk or minimise the effect should the risk event occur. This mitigation process also requires effective communication to ensure that the correct control measures are identified and implemented. An important part of this process can be regarded as the communication to the risk owners who must ensure the implementation of the risk control measures. Finally, effective communication is required during the continuous monitoring process to ensure the effectiveness of each risk component as part of the total risk management process. Therefore, it is essential that the results of each process of the components be communicated because an effective risk management process is dependent on the success of each component's own internal process. In terms of the abovementioned discussion it can be deduced that an embedded operational risk management process is an essential category for effective risk reporting. Based on the aforementioned, it can also be emphasised that risk communication is an essential component of a risk management process. It is directly linked and can ensure the successful execution of the processes involved in each of the risk management components, such as risk identification, risk assessment, risk mitigation and control and monitoring.

Before exploring the concept of operational risk reporting, it is necessary to deal with the broad concept of communication in more detail in order to identify additional categories which can be used as a platform to identity guiding criteria for effective risk reporting.

2.1 Risk communication

Risk communication can be regarded as the process to ensure that the right and timeous information is received by the appropriate individual or group to ensure effective decision-making and implementation of the decisions. In addition, Cleary and Malleret (2006:127) state that risk communication is a process of exchange of information and opinion among individuals, groups and institutions. In order to ensure an effective communication process throughout the organisation, it is imperative to ensure that the right people are involved in terms of generating and receiving information. According to Chapman (2011:245) a business should establish internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk and opportunity management. There should be an open channel to maintain a dialogue with key stakeholders and others to aid the implementation of risk management. Cleary and Malleret (2006:126) state that one reason why risk must be communicated is that there is a need to ensure that the risks identified, assessed and intended to be managed within an enterprise risk management system are properly communicated to the people in the organisation who need to know about them so that they may act. In order to establish a successful risk communication process, it is essential that all the relevant stakeholders be involved and is aware of the process.

According to ISO 31000 (2009:10), the introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation as well as strategic and rigorous planning to achieve commitment at all levels. In this regard, it can be derived that the roles and responsibilities in terms of communication should be clearly defined.

The importance of risk communication is further emphasised by Holmquist cited by Davis (2007:280) when he infers that communication is critical to effective risk management. He (2007: 280-281) mentions several aspects of improving communication that are beneficial to risk managers, such as: managers should be able to quantify the related risks and build suitable controls to ensure that critical information is available and accurate; and risk managers should make information available in a form that is useful to the right people. As such, management should communicate the benefits of risk management to all stakeholders (ISO 31000, 2009).

Effective risk communication will ensure that the right information reaches the right individuals or group to make timeous business decisions. In addition, the ISO 31000 (2009) indicates that an organisation should establish internal communication and reporting mechanisms to support and encourage accountability and ownership of risk. Based on the aforementioned, it is possible to identify the following crucial criteria regarding risk communication which could form part of guiding criteria for risk reporting:

- Timeous and correct risk information is essential.
- Accurate risk information must be channelled to the correct individuals, groups or institutions.
- Internal and external communication and reporting mechanisms should be established.
- Effective risk communication must indicate accountability and ownership.
- Risk communication should enhance dialogue between all stakeholders.
- Risk communication should establish a commitment of all role-players to effective risk management.
- Effective risk communication is beneficial for risk management in terms of:
    - Risk quantification and appropriate risk control measures
    - Ensure the availability of critical risk information for decision-making
    - Accurate and useful risk information to the right target group

In order to add to the abovementioned criteria, each component of the process will be analysed in more detail in terms of risk communication.

2.1.1 Risk identification

Risk identification aims to identify the operational risk exposures of an organisation which could potentially have a negative influence on the business objectives. According to Chapman (2011:159), risk identification is a transformation process where experienced personnel generate a series of risks and opportunities, which are recorded in a risk register. This process requires the analysis of business processes in terms of its objectives and potential inherent risks. As such, this process requires information from various avenues to identify the inherent operational risks. The data required for this process is usually qualitative in nature and can be sourced from, for example, loss incidents, process flow analysis and scenarios. The primary responsibility for the execution of the risk identification process lies with the business owners (who are also the risk owners). The outcome of this process is a risk register of the identified operational risks which is, according to Chapman (2011:162), a key communication tool as it is referred to and incrementally developed throughout the overall risk management process. The risk registers containing the identified risks serves as a platform and input for the next process, namely the risk assessment process.

2.1.2 Risk assessment

Risk assessments can be regarded as the follow-up process from the risk identification process. Croitoru (2014) states that operational risk assessments aim to detect vulnerable operations carried out according to the probability of occurrences and the potential financial impact on the organisation. According to Chapman (2011:197), risk evaluation (assessment) is to assess both the identified risks and opportunities to the business in terms of their aggregated impact on the organisation. Thus, the assessment process involves the analysis of the identified risks (risk register) to determine the potential likelihood and impact of the risks by means of a rating matrix. It furthermore includes the evaluation of risk control measures in place to deal with the identified risks. After evaluating the control measures the rated residual risks are determined. The outcome of this assessment process is an updated risk register consisting of rated risks in terms of probability and impact. The updated risk register, indicating the high-level residual risks can then be used to define the key risk indicators, which can be escalated to responsible persons to manage. Once again, the primary role-players in this process are the business owners. It is also important that this register be communicated to serve as an input to the next process of mitigation and control.

2.1.3 Risk mitigation and control

Various authors view risk control as an important component of a risk management process and it is therefore important to understand this concept. According to Croitoru (2014), risk control is carried out with the aim to transform uncertainties into an advantage for the organisation, limiting the level of threats. Olsen and Wu (2008:73) state that risk control is the activity of measuring and implementing controls to lessen or avoid the impact of risk elements. This can be reactive, after problems arise, or proactive, expending resources to deal with problems before they occur. Young (2014:47) states that risk control involves the application of techniques to reduce the probability of loss. It aims to eliminate or minimise the potential effect of the identified risk exposures. In addition, Chapman (2011:294) states that the controls need to be meaningful in terms of significant issues or events, and relate to the key business objectives. He (2011:294) also, states that timely controls are necessary so that there is sufficient time to act before negative events turn into terminal events.

Based on the aforementioned, it is apparent that the control component of an operational risk management process is crucial to either prevent a loss from occurring or to minimise the effect should such an event occur. It is also clear that to be proactive, it is essential that timeous decisions are made at the right management levels. In order for management to make these decisions, they must be provided with the correct and accurate information, which they can obtain by means of an effective risk communication process. This process should involve appropriate risk reports. Olson and Wu (2008:73) state that risk reporting communicates identified risks to others for discussion and evaluation. According to Blunden and Thirlwell (2013:25), reports on risk should be linked to relevant controls and actions so that recipients can use them to remedy control failures, review risk appetite and perhaps remove controls. Cleary and Malleret (2006:127) state that risk reporting is essential in making decisions. It, furthermore, enables people to participate in deciding how risks should be managed; is a vital part of implementing decisions; and informs and advises people about risks. In addition, it is stated that operational risk reports play a key role in clearly identifying the operational risk strategy and how to achieve it (Blunden and Thirlwell, 2013:152 – 155).

Risk control as a component of a risk management process can also be regarded as the final step in the finalisation of the risk register, which will then include the rated control measures and the residual risk exposures which should be managed according to its rating. However, it is important to note that risk management is a dynamic process and the risk register should be updated according to changing circumstances. Therefore, it is essential that a continuous risk monitoring process should form part of an operational risk management process.

2.1.4 Risk monitoring

According to Dowd, cited by Alexander (2003:46), the result of the identification and assessment process is likely to generate a number of indicators through which operational risk may be monitored on an ongoing basis. If operational risk is to become embedded within a risk management culture of the organisation, then monitoring should be conducted on a frequent and regular basis. According to ISO 31000 (2009), both monitoring and review should be a planned part of the risk management process and involve regular checking or surveillance.

Chapman (2011:234) states that the primary goal of monitoring is to monitor the performance of risk response actions to inform the need for proactive risk management intervention. The monitoring and review process will be sufficient when it has satisfied the following sub-goals:

- Early warning indicators have been developed.
- Internal and external context are monitored to establish the current analysis of opportunities and risks.
- Risk actioners and managers are implementing the risk and opportunity responses for which they are responsible in a timely manner.
- Risk register are regularly updated in terms of actions.
- Reports are issued on a regular cycle, providing visibility of the progress made in the success or otherwise of the risk management actions.
- Contingencies are revised to reflect the current risks, opportunities and their assessment.

In addition and according to ISO 31000 (2009), the organisation's monitoring and review processes should encompass all aspects of the risk management process for the purposes of:

- ensuring that controls are effective and efficient in both design and operation;
- obtaining further information to improve risk assessment;
- analysing and learning lessons from events, changes, trends, successes and failures;
- detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and
- identifying emerging risks.

According to Cleary and Malleret (2006:79), management must ensure that it has effective procedures in place to monitor the events giving rise to the risks it has accepted, so that it has early warning of changes that suggest that the risk is increasing, and that these observations are communicated rapidly to officials who can make proper decisions about how to deal with the changes. It is clear that monitoring plays a crucial role during the operational risk management process. However, it is essential that communication by means of risk reports should be embedded in the process.

According to ISO 31000 (2009), the results of monitoring and review should be recorded and externally and internally reported as appropriate, and should also be used as an input to the review of the risk management framework. In addition, Dowd (2003:46) states that it is expected that these reports should cover the results of monitoring activities, such as trend analysis and compliance reviews.

In order to provide more clarity on risk reporting, the next section will analyse the concept in more detail.

2.2 Risk reporting

Risk reporting can be seen as one of the more important aspects of risk management in order to effectively communicate various risk information to stakeholders. Haubenstock, cited by Alexander (2003:253) states that reporting should satisfy the requirements of individual business managers as well as offering a consolidated view for senior management. A key objective is to communicate the overall profile of operational risk across all business areas and types of risk. Ong (2007: 627) states that the objectives of management reporting are to inform management about their operational risk experience, trigger actions and resource allocations where necessary, and assure management about the effectiveness of the risk management process. Hain (2009:285) states that sound operational risk management critically depends on the support of employees and their willingness to provide adequate and true information. As such, risk reporting plays a crucial role in risk management and internal and external risk reporting is vital to ensure the provision of adequate and accurate risk information for decision-making and risk management. Olsen and Wu (2008:73) state that risk reporting communicates identified risks to others for discussion and evaluation. According to Chapman (2011:342), risk reporting is a sub-goal of communication and reports must be prepared on a regular basis advising of changes to the risk exposure and the degree of success being realised by risk response activities. Dowd (2003:46) states that an organisation must implement a system of internal reporting of operational risk with the reporting mechanism geared to the needs of the end user. This is essential if the organisation's operational risk policy is to be established and evaluated.

According to Dowd (2003:46), the board of directors should receive enough information to understand the organisation's overall operational risk profile and its material risks. Once senior management receives risk reports they will be able to become involved in operational risk management and make appropriate risk decisions. Blunden and Thirlwell (2103:33) state that good operational risk reporting will also generate management involvement and consensus, which will drive the ongoing identification, assessment and control of operational risk. It is clear that risk information is not only an upward reporting process, but also requires a top-down communication. In this regard Dowd (2003:46) state that reporting should not be viewed as a one-way street, with information only being passed upwards, equally important is downward dissemination or feedback. In addition, Croitoru (2014:29) states that the organisation must ensure that adequate information flow both vertically and horizontally. However, it is crucial that the risk information flowing from top-down and bottom-up should be adequate and sensible in order to lead to decisions or actions. In this regard Blunden and Thirlwell (2013:23) infer that risk reports and the information in them should lead to action. The key to good reporting is to tailor it to the needs of the reader at every management level. In addition and according to COSO (2004:33), reliable reporting provides management with accurate and complete information appropriate for its intended purpose and should support management's decision-making and monitoring of the organisation's activities and performance.

It is clear that the flow of operational risk information is crucial for effective risk reporting. This information should stem from the operational risk management process and can be generated from the applicable methodologies. According to Girling (2013: 234), reporting will usually include analysis of internal loss data, external loss data, risk and control self-assessment results, scenario analysis results and capital. In order to quantify and qualify the operational risk exposures, the following popular methods (also mentioned in the New Basel Accord (Basel II 2003)) can be used (Young 2014a):

- *Loss history*. This methodology involves the use of loss data (external and internal) to identify the risks based on events that happened in the past which can be used to avoid or manage similar risk incidents. Haubenstock (2003:256) states that events are the operational losses (internal and external) that provide the historical base for risk analysis and quantification. The primary report is a summary of statistics from the losses indicating trends of total losses and mean average losses. Reporting often includes any relevant external losses, industry trends or news related to regulation, competitors or other risk factors that might be of interest. Reports on loss data can be used as an input to determine the inherent risks of an organisation when compiling the risk register. Information can also be reported by means of an incident report, reflecting the detail of a loss incident such as the detail on what occurred, those involved and the actual loss.

- *Risk and control self-assessments (RCSA).* According to Young (2014), this method is a bottom-up approach to evaluate operational risk. Self-assessments are performed by the business areas and results are aggregated to provide a qualitative profile of risk across the organisation and related action items. The results are communicated with a combination of risk maps, graphic results, issues and initiatives (Haubenstock, 2003:253).The self-assessment process involves the identifying and rating of the inherent risks and existing control measures in order to determine the residual risks that are critical to be managed. This method focuses on potential future risk exposures that should be managed and the results of the RCSA process can be reported on and incorporated into the risk register. It can furthermore form the basis for determining the key risk indicators.
- *Key Risk Indicators (KRIs).* The identification of KRIs can result from the RCSA process and should be managed on a regular basis in order to focus on the current risk exposures and to serve as an early warning of a potential risk incident to management. According to Haubenstock (2003:256), key risk indicators may also be reported, including related escalation criteria, explanations of any excesses and identified trends. Many KRIs are customised at a business unit level, but some may be common and reported in a consolidated fashion. Davis (2007: 7) cited Grandfield who stated that KRIs are not the only component of risk reporting; there are a large number of data elements that need to be combined to make some meaningful picture of the overall risk landscape for a business, such as: current issues and status of risks; audit and regulatory examinations; and key initiatives. However, seeing that KRIs focuses on the current risk exposures, it is crucial that regular risk reports be generated to the appropriate management levels to make decisions should a pre-set threshold be breached or a trend of an increase in risk is determined. Haubenstock (2003:253) states that reporting communicates the overall level of risk and highlights key trends or exceptions that may require particular attention. Typical reports in this regard could include various forms of graphs.
- *Scenarios*. The use of scenarios involves the expert opinions, concerns and experience of key role-players in the organisation to identify potential threats and risk exposures for the organisation (Young 2014). Reports on the scenarios on future potential risks can serve as an input for the risk register.

It is apparent that the operational risk methodologies play an important part in internal risk reporting. According to Girling (2013:219 – 220), there are many ways to ensure that the reporting drives action and to protect against the danger of producing worthless reports and the abovementioned methodologies can be used in this regard. However, it is crucial that the reports reach the right management level (manager) to ensure timely and adequate decisions; appropriate actions; and to ensure an updated operational risk profile. In order to ensure the operational risk profile, it is important that there is an integrated approach to the reports from each risk methodology. This is illustrated in Figure 2. Cleary and Malleret (2006:204) state that an integrated approach between risk assessment, risk management and risk communication is essential. For a variety of reasons, many large organisations and the people who succeed in them, are often much better at analysis, measurement and the formal processes of management than they are at communication. As such it is imperative to explicitly define the processes which will ensure an integrated operational risk reporting approach.

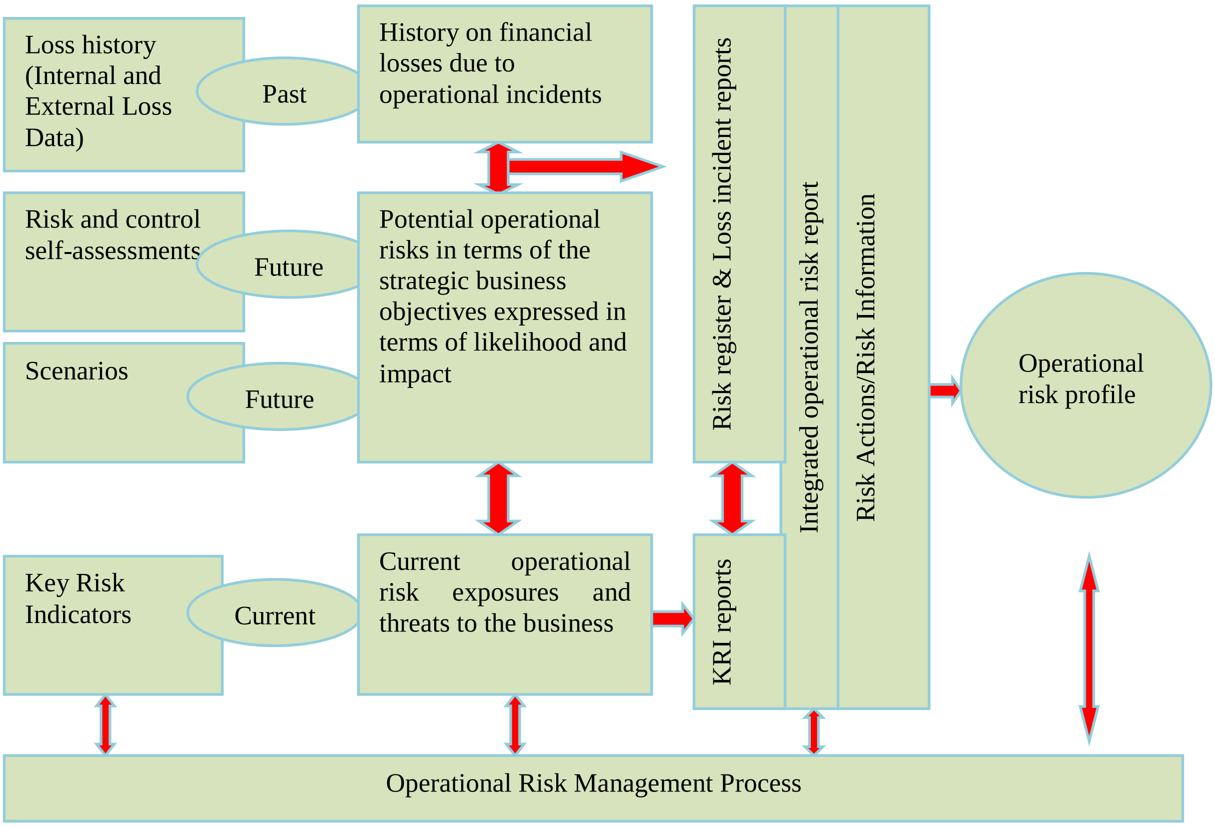
The diagram (Figure 2), illustrates that during the operational risk management process, the loss history (internal and external loss data), Risk and Control Self-Assessments (RCSA), and Scenarios can be used to determine the past and future risk exposures, resulting in a risk register and incident reports. The KRIs can be determined from the risk register and can be managed to determine the status of the current risks and serve as early warning of potential loss incidents. By means of an integrated reporting process, the risk information can be used to determine the operational risk profile. However, according to ISO 31000 (2009), relevant information must be derived from the application of risk management and should be available at appropriate levels and times; and there should be processes in place for consultation with internal stakeholders. It is therefore necessary to identify responsible individuals who must either compile the risk reports or to take the necessary actions/decisions. The risk profile is an essential result of the risk management process and could serve as an input for various activities such as the business planning process, annual business reports and a general view of the organisation’s operational risks.

According to ISO 310000 (2009), responsibilities for risk management should be clearly defined. Blunden and Thirlwell (2013:152 – 155) state that any risk report should enable management to take ownership of the information. They (2013:23), also add that risk ownership and control ownership can be clarified through good reporting and assist in identifying priorities for enhancing controls and the organisation’s operational risk profile.

In terms of the ISO 31000 (2009), an organisation should establish internal communication and reporting mechanisms which will support and encourage accountability and ownership of risk. These mechanisms should ensure that: there is adequate internal reporting on the framework, its effectiveness and the outcomes; relevant information derived from the application of risk management is available at appropriate levels and times; and that there are processes for consultation with internal stakeholders.

According to Bolton and Berkey, cited by Davis (2005:238), there should be regular reporting of pertinent information to senior management and the board of directors. In terms of regular reporting, Blunden and Thirlwell (2013:152 – 155) state that operational risk reporting is a continuous evolving process due to the dynamic nature of good risk reporting. Haubenstock (2003:253) states that reporting is necessary for all levels of the organisation, but the exact content and frequency of the information must be tailored to each business area. In this regard, Dowd (2003:46) states that in general the board of directors should receive higher-level information. However it is important that the risk information makes sense and is applicable for decision-making. According to ISO 31000 (2009), decision makers at all levels of the organisation, should ensure that risk management remains relevant and up-to-date. Alexander (2003:23) cited Swenson (2003:23) cited by Alexander, mentioned that there must be regular reporting of relevant operational risk data to business unit management, senior management and the board of directors and that the board and senior management must be actively involved in the oversight of the operational risk management process.

Figure 2. Integrated reporting from operational risk methodologies


Loss history (Internal and External Loss Data)
Past
History on financial losses due to operational incidents
Risk and control self-assessments
Future
Scenarios
Future
Potential operational risks in terms of the strategic business objectives expressed in terms of likelihood and impact
Risk register & Loss incident reports
Integrated operational risk report
Risk Actions/Risk Information
Operational risk profile
Key Risk Indicators
Current
Current operational risk exposures and threats to the business
KRI reports
Operational Risk Management Process

On the other hand, risk reporting mechanisms should also cater for external stakeholders and should incorporate formal risk disclosure processes. It is important to establish an external reporting process or disclosure to ensure that relevant risk information regarding an organisation's risk profile reaches all stakeholders. Hain (2009:291) states that gathering risk information and communicating it inside the institution supports effective risk management, allows for the consideration of risk in business decisions and is the basis for reporting the firm's operational risk to stakeholders. Cleary and Malleret (2006:204) state in this regard that it must be ensured that relevant information are communicated in appropriate ways both to the people who are responsible for dealing with the threat and to those outside the firm who may be affected by it. However, it is important that risk information which is reported to external stakeholders is considered in terms of the sensitivity of the information, in order not to compromise the competitiveness or the reputation of the organisation. According to ISO 310000 (2009), the organisation should develop and implement a plan as to how it will communicate with external stakeholders. This should involve:

- engaging appropriate external stakeholders and ensuring an effective exchange of information;
- external reporting to comply with legal, regulatory, and governance requirements;
- providing feedback and reporting on communication and consultation;

- using communication to build confidence in the organisation; and
- communicating with stakeholders in the event of a crisis or contingency.

Disclosure of operational risk to external parties should be carefully monitored, because different stakeholders require different risk information. Hain (2009:288) states that the motivation of external parties regarding monitoring corporate decisions differs among stakeholders. For example regulatory authorities focus on social welfare, the capital market requires information for investment decisions, insurance companies try to calculate fair premiums and rating agencies as well as public accounting firms assess firms as part of their business. AIRMIC (2010:16) states that external risk reporting should be designed to provide external stakeholders with assurance that risks are being adequately managed.

In addition Hain (2009:288) states that higher transparency leads to improved risk management of the firm. According to Phillips (2010:36), risks are best managed when information is transparent – that is, timeously and widely available to those who need it. According to ISO 31000 (2009), risk management should be: transparent; appropriate; and ensure the timely involvement of all stakeholders. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria. Bolton and Berkey (2005:238) state that banks, for example, should make sufficient public disclosure to allow market participants to assess their approach to operational risk management. Furthermore, AIRMIC (2010:16) concludes that risk disclosure is a more forward-looking activity that could anticipate emerging risks.

From the aforementioned it is apparent that internal and external risk reporting should be an intrinsic part of an operational risk management process.

In order to ensure a streamlined operational risk reporting process and based on the aforementioned literature review, it is possible to identify guiding criteria, which are stipulated in the next section.

3 Guiding criteria for operational risk reporting

The guiding criteria for operational risk reporting aim to assist organisations in managing operational risk and to ensure that it adds value. A non-exhaustive list of guiding criteria for risk reporting can be sorted into the following main categories:

- Risk management process to generate appropriate risk reports (Risk identification, risk assessment, risk control).
- Governance.
- Internal risk communication.
- External risk communication and disclosure.
- General characteristics of sound operational risk reports.

Derived from the literature, the criteria for operational risk reporting are included in Table 1 grouped per category.

In order to substantiate the applicability of the guiding criteria identified in this article, a survey was undertaken to confirm the criteria for operational risk reporting and to determine the current status of risk reporting assessed against these criteria.

4 Research methodology

In order to confirm the appropriateness of the identified guiding criteria for operational risk reporting, it was decided to identify a group of respondents from the Guideline Biztech database who are involved in risk management projects across various industries and sectors who mainly operates at middle and top management levels. The Guideline Biztech database holds information on a variety of risk-related projects as well as those involved in these projects. As such, it can be reasonable accepted that these individual role-players have a good understanding ad knowledge of risk management.

The data was collated by means of a closed questionnaire which was distributed electronically as well as physically to pre-identified role-players involved in operational risk management. The target population was identified at the following management levels: member of the board of directors, executive management, business management, risk management, compliance management, internal audit and financial management. The main reason for distributing the questionnaire to the aforementioned was that these positions can be regarded as the main role-players in an organisation's risk management processes.

The aim of the questionnaire was, firstly, to determine the appropriateness of the guiding criteria for operational risk reporting and to determine the current status of each criterion to ensure a streamlined risk reporting process. The questionnaire requested respondents to indicate on a 5-point Likert scale their views and experiences regarding specific questions on the identified criteria for operational risk reporting and to indicate its current use. The response was analysed in terms of descriptive statistics according to the following scale:

1. To no degree
2. To some degree
3. To a moderate degree
4. To a degree
5. To a full degree

Table 1. Criteria for operational risk reporting

Category	***Criteria***
Risk management process	• Qualitative risk data is required for risk identification sourced from loss incidents, risk and control self-assessments, key risk indicators and scenarios. • Risk reporting should include the overall operational risk profile of the organisation, based on the results of the operational risk methodologies. • Continuous monitoring and risk reports are essential for proactive risk management. • Risk reports during the risk monitoring process should report on the effectiveness of risk controls. • Risk reports should include information on internal and external operational risk losses. • Risk reports should indicate potential risks derived from risk and control self-assessments. • Risk register forms the basis for risk assessments. • Risk reports should include risk trends to serve as early warning as part of a key risk indicator management process. • Risk reports should provide assurance to management about the effectiveness of the operational risk management process. • Risk reports should indicate potential operational risks derived from scenarios. • Risk reports should result from an efficient internal risk communication process.
Governance	• Risk reporting process should be included in the organisation's risk management policy. • Business owners should be responsible for operational risk management and reporting process. • Risk reporting is essential for decision-making. • Risk reporting mechanisms should indicate accountability and ownership of risks. • Risk reporting should include a bottom-up dissemination of operational risk information. • Risk reporting should include a top-down communication of feedback and decisions.
Internal risk communication	• There should be a system of internal risk reporting. • Risk reporting should ensure high-level risk information to the board of directors.
External risk communication	• Risk reporting should cater for external disclosures on operational risks to stakeholders. • External risk reporting should include relevant information to support stakeholders in business decisions regarding the organisation. • External risk reporting should comply with legal, regulatory and governance requirements. • External risk reporting should be customised according to the needs of different shareholders. • Risk reports to external stakeholders must not compromise the competitiveness and reputation of the organisation.
Characteristics of sound Risk reports	• Effective proactive risk management decisions should result from reliable, accurate and appropriate risk reports. • Risk reports should be issued on a regular cycle in order to monitor risk management actions. • Risk reports should be internally and externally available. • Risk reporting should be informative on operational risks. • Risk reporting should be based on adequate and true information. • Risk reporting is a continuous process. • Risk reporting should be flexible and allow for customisation to suit the needs of the receiver of the risk information. • Risk reports should include relevant controls and actions. • Risk reports should include resource allocations. • Risk reports should include information that will ensure revision of risk treatments.

5 Research results

The questionnaires were randomly distributed to various role-players listed on the database who were indicated as middle and senior management involved in risk management across a variety of industries and business sectors in South Africa. A total of 85 questionnaires were distributed and 45 were returned on the due date which represents a 52.9% response which is acceptable for analysis purposes using a descriptive statistical approach. Those members who responded reside from a variety of business sectors in South Africa and are indicated in table 2 below:

Table 2. Business sectors of respondents

Business sector	*Response percent*	*Response count*
Banking	11.1%	5
Financial Services	6.7%	3
Government Departments	8.9%	4
Insurance	6.7%	3
Other	66.6%	30
Total	100%	45

Although most of the respondents reside from other sectors than those specifically listed, it can be deduced that operational risk management are being managed in a variety of business sectors, such as municipalities, education, mining, agriculture and consulting firms. Eleven per cent of the respondents are from the banking sector which can be regarded as one of the leading business regarding the management of operational risk in South Africa, mainly due to the implementation of the Basel guidelines, which were adopted by the South African Reserve Bank.

Figure 3 indicates the positions of the respondents, while Figure 4 indicates the years of experience.

Sixty per cent of the respondents fall in the top management and business management categories, indicating that most respondents should be familiar with risk reporting and should know the role and responsibilities of top management. According to the years of experience, 55.5% of the respondents have more than 10 years' experience, while 31% have between 5 to 10 years' experience, indicating a vast level of experience in the relevant organisations and exposure to risk management and reporting.

Figure 3. Positions of respondents

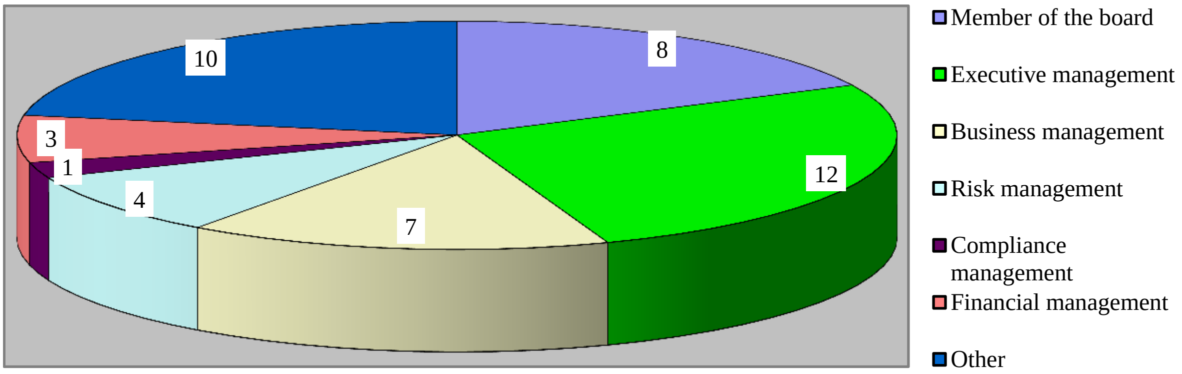
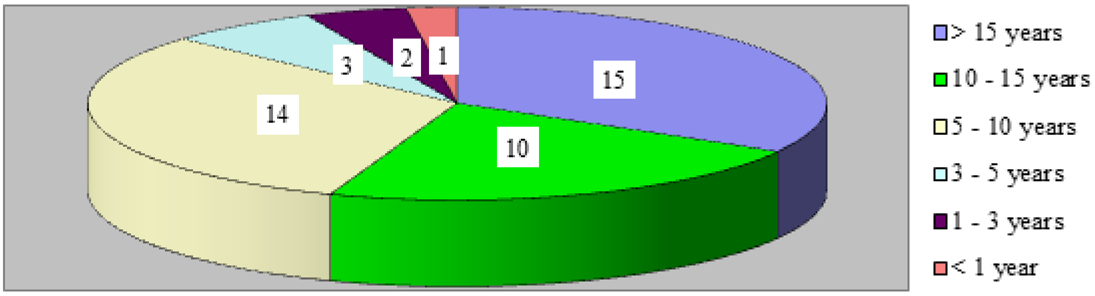


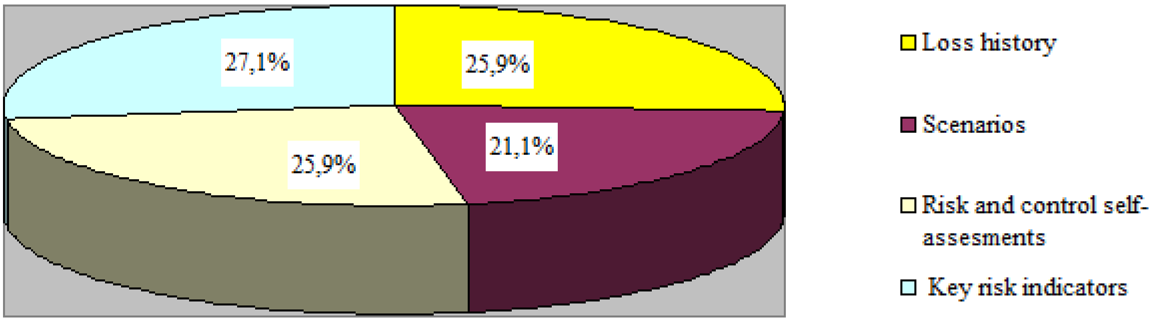
Figure 4. Years of experience



According to the feedback 74% of the respondents indicated that operational risk is being managed as an independent risk type in their organisation, while 26% indicated that it is still managed to a moderate degree. It can therefore be derived that operational risk is being managed by most organisations as an independent risk type which confirms the importance of managing it according to a structured approach and process. The inclusion of an operational risk reporting process in an operational risk management policy, however, seems to still be at a developmental level. Thirty-five per cent of the respondents indicated that the risk reporting process is included into the risk policy to a moderate degree, while 17% indicated that it is incorporated to a degree. Forty-eight per cent responded to the adequacy of the risk reporting process being incorporated into an operational risk management policy. It can therefore be assumed that although most organisations manage their operational risk as an independent risk type, the actual reporting process still requires attention in order to ensure an adequate reporting process.

According to the respondents the basic operational risk management tools are being used to manage operational risk. Figure 5, indicates the response in terms of the agreement that the respective tools are being used at an acceptable level. The response indicates that the use of KRIs seems to be the most popular (27.1%) followed by loss history (25.9%) and risk and control self-assessments (25.9%), with scenarios at 21.1%.

Figure 5. Use of operational risk management tools



In order of priority, the respondents indicated that the use of KRIs is the most significant, followed by risk and control self-assessments, loss history and scenarios. The most important deduction regarding the response is that all respondents indicated the use of these tools to manage operational risk. In the literature review, it was also determined that these tools are pertinent to provide information for an effective operational risk reporting process.

According to the response 79% agreed that a KRI management process provides risk trends which could serve as early warning during operational risk reporting. Therefore most of the respondents indicated that KRIs are used during the risk reporting process. The literature indicated that the use of KRIs to identify risk trends and to serve as early warning during the management of operational risk is an important part of risk management. As such, it can be reasoned that although some organisations indicated that KRIs are the most popular risk management tool, it still requires some development in terms of its actual benefits such as trend analysis and early warning.

Sixty-three per cent of the respondents indicated that the use of scenarios to indicate potential risks is to no degree or to a moderate degree being used for risk management and reporting. Only 5% indicated that scenarios are adequately used as an operational risk management tool. Therefore, it can be deduced that most organisations are aware of the use of scenarios as an operational risk management tool; however, it can still be exploited in terms of its benefit to proactively identify operational risk exposures for an organisation.

On the other hand, 58% of the respondents indicated that risk and control-self-assessments are used to report on potential operational risks. Twenty-one per cent of the respondents indicated that it is used to a moderate degree. As such, it can be assumed that risk and control self-assessments play a crucial role in operational risk management and reporting. According to the response, 79% indicated that a risk register is compiled from an operational risk identification and assessment process. It can thus be readily accepted that risk registers are being compiled as a result of an operational risk management process which is in itself an important risk communication tool as indicated in the literature review.

Seventy-nine per cent of the respondents indicated that operational risk reports are used to report on internal and external risk losses. According to the literature, risk reports should include information on losses suffered as it serves as the basis to determine the inherent risk exposures which should be managed as part of the risk management process. In this regard, it can be concluded that operational risk reports still requires attention to ensure the adequate reporting on internal and external losses. A reason for this lack of adequacy in reporting might be that organisations are not reporting all losses due to a potential negative influence on their reputation. However, this situation could hamper the effectiveness of operational risk management and negatively influence sound decision-making when top management relies on accurate risk reports to make these decisions. It is therefore imperative that all risk losses be reported accurately and timeously to serve as an input during the risk management and decision-making process.

Respondents indicated a 42% agreement that risk reports include a report on the effectiveness of risk control measures, 26% to a full degree and 32% to no or some degree. It can therefore be deduced that risk reports do not adequately report on information relating to risk control measures. In terms of the literature review, it is important that risk mitigation be communicated to risk owners who must ensure the implementation of the risk control measures. Therefore it seems that risk reports still require attention in order to include risk control measures to ensure effective risk management.

Fifty-two per cent of the respondents indicated that risk reports provide assurance to management on the effectiveness of the operational risk management process. It can thus be deduced that according to 48% of the response, risk reports can be improved to provide the assurance to management that the operational risk management process actually contributes to the effectiveness of operational risk management. On the other hand, 78.9% of the respondents indicated that risk reports provide an operational risk profile of the organisation. This could indicate that risk reports mostly concentrate on the overall results of the operational risk methodologies instead of detail information. In order for management to make decisions, it is necessary to include detail information instead of only an overall risk profile in order to support management decisions in terms of risk management. Although, it is essential for risk reports to provide the overall operational risk profile of the organisation, it is required that risk reports should include various levels of detail for different management levels. According to the literature, business managers are the risk owners and should be responsible for the risk and reporting process. Eighty-eight percent of the respondents indicated that business owners are responsible for risk management and the reporting process to a moderate and full degree. Therefore, it can be accepted that the risk reporting process is an important responsibility of business owners. On the other hand the 83.4% of the respondents also indicated that risk managers are to a degree responsible for the risk management and reporting process. It is clear that there is a dual responsibility regarding the risk management and reporting process between business managers and risk managers, although the emphasis should differ. Business managers should be ultimately responsible for risk management, while risk managers play a supporting role to ensure the effectivity of the risk management and reporting process.

Although internal audit plays an important role in providing assurance that the risks are being managed, they play a limited role in the actual reporting of risks. This is supported by 61.1% of the response that indicated that internal audit is to a lesser degree involved in risk reporting. However, it seems that some organisations (38.9%) do involve internal audit in the risk reporting process. Although this approach is not the ideal, it seems that some smaller organisations depend on the expertise of internal auditors to assist in the risk reporting processes.

According to the response, 77.8% agreed that risk reports result from an efficient risk communication process. Therefore, it can be confirmed that an efficient risk communication process should be embedded in an organisation to ensure adequate risk reports. Eighty-three per cent of the response indicated that a system of internal risk reporting is embedded in the organisation, emphasising the importance of a risk reporting system. In addition, 88.9% of the respondents indicated that risk reporting is essential for decision-making. Similarly, 88.8% of the respondents agreed that risk reporting is essential for proactive risk management.

Regarding the bottom-up dissemination of operational risk information, 66.7% of the respondents indicated that the process is inadequate or only effective at a moderate degree. Thirty-three per cent of the respondents indicated that the process is adequate. It can therefore be deduced that although the bottom-up reporting process to disseminate operational risk information is in place, it still requires attention to ensure the development of an adequate reporting process. On the other hand, 50% of the respondents agreed that a top-down risk communication process includes feedback and decisions by top management, 33.3% indicated that it is at a moderate degree. As such, it seems that the top-down communication of risk management feedback and decisions is more embedded than the bottom-up risk reporting of information. However, from the response 88.8% of the respondents agreed to a degree that risk reports contain high-level risk information to the board of directors. This indicates that although the risk information from a bottom-up approach still requires attention, the reports to the board of directors are adequate. Therefore, it can be deduced that risk reporting still requires attention in terms of detailed operational risk information. Seventy-seven per cent of the respondents agreed that the operational risk reports provide information concerning regulatory and compliance information. In addition, 94.5% of the respondents agreed that operational risk reports comply with legal, regulatory and governance requirements. Similarly, 88.9% of the respondents agreed that operational risk reports cater for disclosures on risk management to stakeholders. In this light, it can be deduced that operational risk reports are mostly driven by regulatory and compliance requirements as well as general risk information for disclosure purposes and could still be expanded to include more management information to enhance internal business decision-making.

Regarding the inclusion of operational risk information in risk reports to support stakeholders to make business decisions, 83.3% of the respondents agreed to its importance. This response emphasises the importance of including relevant operational risk information disclosed to stakeholders that will assist effective business decisions. However, it is imperative that external operational risk reports should not compromise the organisation’s competitiveness and reputation as indicated by 87.6% of the respondents.

The rating of the criteria for operational risk reports is indicated in Figure 6. According to the response all the criteria were rated as applicable for effective operational risk reporting. The criterion that was rated the highest was the inclusion of information that will ensure revision of risk treatments, followed by the criterion to ensure that operational risk reports must be based on adequate and true information. This is followed by the criterion that there must be ensured that risk reports must include relevant controls and actions. Risk reporting as a continuous process is the next important criterion, followed by the inclusion of resource allocations. It is clear that the first five criteria for effective risk reporting, relates to adequate information, which reflects controls and actions on a continuous basis. As such it can be deduced that according to the response, there is a need for operational risk reports at a lower level which could add value to the actual management of operational risks.

Figure 6. Rating of criteria for operational risk reports

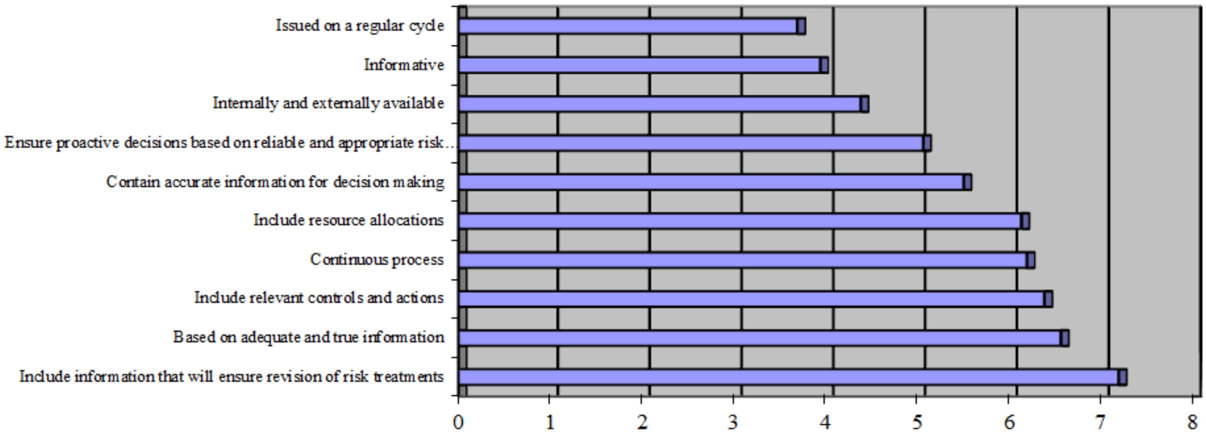


Table 3. Checklist to evaluate operational risk reports

#	*Guiding criteria*
1	Operational risk reporting should be incorporated into the organisation's operational risk policy.
2	Operational risk reporting mechanisms should indicate accountability and ownership of risks.
3	Operational risk reporting should assure management about the effectiveness of the operational risk management process.
4	Operational risk reports should be based on adequate and true information.
5	Operational risk reporting should be informative on operational risks.
6	Operational risk reports should provide adequate and accurate risk information for decision-making.
7	Operational risk reporting should trigger actions and resource allocations.
8	Operational risk reporting should communicate the risk profile of operational risk to all business areas.
9	Operational risk reports should include potential risks which were derived from the risk methodologies (Risk and control self-assessments; loss history, key risk indicators and scenarios) and illustrate the risk profile of the organisation.
10	Operational risk reporting should be a continuous process to ensure regular risk reports.
11	Operational risk reporting should include a bottom-up dissemination of operational risk information.
12	Operational risk reporting should include a top-down communication of feedback and decisions.
13	Operational risk reports to external stakeholders must not compromise the competitiveness and reputation of the organisation.
14	Operational risk reporting should be flexible and allow for customisation to suit the needs of the receiver of the risk information.
15	Operational risk reporting should ensure high-level risk information to the board of directors.
16	External operational risk reporting should comply with legal, regulatory and governance requirements.
17	External operational risk reporting should include relevant information to support stakeholders in business decisions.
18	Operational risk reporting should ensure the revision of risk treatment.

In conclusion to the empirical analysis of the response, the guiding criteria for effective operational risk reporting, identified by the literature review, became evident.

6 Conclusion

This study provided some insights on risk reporting as an essential part of an operational risk management process. During the literature review it became evident that operational risk reports should add value and form part of an integrated reporting approach. It also became clear that operational risk reports stem from the operational risk management methodologies implemented during a risk management process to identify, assess, mitigate and control and monitor operational risks. The use of these methodologies namely: risk and control self-assessments; key risk indicators; loss history; and scenarios proved to be vital for the effective communication of risk information.

The primary conclusions drawn from the empirical analysis can be summarised into a non-exhaustive checklist that could serve as a guideline to evaluate the effectiveness of operational risk reports for corporate organisations (Refer to Table 3).

The abovementioned guiding criteria could add value to address current uncertainties on operational risk reporting and therefore also addresses the research question of this article namely: are there clear guideline criteria for operational risk reporting as an input to an integrated reporting process? To address this research question, the purpose of the article was to provide guiding criteria for effective operational risk reporting, based on a literature review, to add value to a proactive approach to operational risk reporting. The criteria can also be used to ensure that operational risk reports are effective, achieve its objective and reach the right target audience. Effective operational risk reports, based on the guiding criteria, can all add value by serving as an input for integrated reporting, a concept currently being widely researched.

References

1. Association of Insurance and Risk Managers (AIRMIC). 2010. A Structured Approach to Enterprise Risk Management. www.airmic.com (1-18).
2. Australian/ New Zealand Standard: Risk Management. Joint Technical Committee OB-007. 3rd Edition, 21 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. 2006. International Convergence of Capital Measurement and Capital Standards: A Revised Framework. Bank for International Settlements.
5. Blunden, T & Thirlwell, J 2010. *Mastering Operational Risk: A practical guide to understanding operational risk and how to manage it.* 1st edition. Edinburgh: Pearson.
6. Bolton, N & Berkey, J. 2005. Aligning Basel II Operational Risk and Sarbanes-Oxley 404 Projects. Operational Risks: Practical Approaches to Implementation. Edited by Davis E. Published by Risk Books, a Division of Incisive Financial Publishing Ltd. Haymarket House.
7. Chapman, RJ. 2008. Simple tools and techniques for enterprise risk management. John Wiley & Sons Ltd. West Sussex, England.
8. Chapman, RJ. 2011. Simple tools and techniques for enterprise risk management. 2nd Edition. John Wiley & Sons Ltd. West Sussex, England.
9. Cleary, S & Malleret, T. 2006. Resilience to Risk. Business success in turbulent times. Human & Rousseau, A Division of NB Publishers (Pty) Ltd. Pretoria.
10. Committee of Sponsoring Organizations (COSO) of the Treadway Commission. 2004. Enterprise Risk Management – Integrated Framework.
11. Dowd, V. 2003. Measurement of Operational Risk: the Basel approach. Operational Risk. Regulation, Analysis and Management. Edited by Alexander, C. Pearson Education Ltd. Harlow.
12. Eccles R., Krzus, MP, & Tapscott, D. 2010. One Report: Integrated Reporting for a Sustainability Strategy. Wiley Publishers. 1st Edition.
13. Girling, P. 2013. Operational Risk Management. A complete guide to a successful operational risk framework. John Wiley & Sons, Inc. New Jersey.
14. Grandfield, A. 2005. Operational Risk Management – The View from the Trenches. Operational Risk. Practical Approaches to Implementation. Edited by Davis, E. Published by Risk Books, a Division of Incisive Financial Publishing Ltd. Haymarket.
15. Gregoriou, G.N. 2009. Operational Risk Toward Basel III. Best practices and issues in modelling, management and regulation. John Wiley & Sons, Inc, New Jersey.
16. Hain, S. 2009. Managing Operational Risk: Incentives for reporting and disclosure. Journal of Risk Management in Financial Institutions Vol 2, 3 284-300. Henry Stewart Publications.
17. Haubenstock, M. 2003. The operational risk management framework. Operational Risk. Regulation, Analysis and Management. Edited by Alexander, C. Pearson Education Ltd. Harlow.
18. Holmquist, E. 2007. Operational Risk. Driving Value Creation in a Post-Basel II Era. Operational Risk and Communication Conduits. Edited by Davis, E. Published by Risk Books, a Division of Incisive Financial Publishing Ltd. Haymarket.
19. King III. 2009. King Report on Governance for South Africa. Institute of Directors in Southern Africa (IOD), Pretoria.
20. ISO 31000. 2009. Risk Management – Principles and Guidelines. International Organization for Standardization, Geneva. pp. 8 – 21.
21. James, ML. 2014. The Benefits of Sustainability and Integrated Reporting: An investigation of accounting majors' perceptions. Journal of Legal, Ethical and Regulatory Issues. Volume 17, Number 2, 2014 (92 – 113).
22. King, M. 2014. Transforming Corporate Reporting. Internal Auditor. April 2014 (58 – 62).
23. Makiwana, TS & Padia, N. 2012. Evaluation of Corporate Integrated Reporting in South Africa Post King III Release South Africa – an exploratory enquiry. Journal of Economic and Financial Sciences | JEF | July 2013 6(2), pp. 421-438.
24. Ong, M. 2007. The Basel Handbook. A guide for financial practitioners. Published in Association with KPMG by Risk Books, a division of Incisive Financial Publishing Ltd. Haymarket.
25. Olson, DL & Wu, DD. 2008. Enterprise Risk Management. World Scientific Publishing Co. Pty. Ltd. Singapore.

26. Phillips, K. 2010. Transparency creates accountability. Corporate Governance. Enterprise Risk October 2010 (36).
27. Swenson, K. 2003. A qualitative operational risk framework: guidance, structure and reporting. Operational Risk. Regulation, Analysis and Management. Edited by Alexander, C. Pearson Education Ltd. Harlow.
28. Verschoor, C.C. 2014. Integrated Reporting: Lags in the U.S. Strategic Finance, December 2014. Institute of Management Accountants.
29. Young, J. 2014. Operational Risk Management. 2nd Edition. Pretoria. Van Schaik Publishers.
30. Young, J. 2014a. Practical Guidelines to Formulate an Operational Risk Appetite Statement for Corporate Organisations: A South African Perspective. Journal: Corporate Ownership and Control. Sumy, Ukraine. Volume 12, Issue 1, Autumn 2014 (47 - 63).