THE USE OF KEY RISK INDICATORS BY BANKS AS AN OPERATIONAL RISK MANAGEMENT TOOL: A SOUTH AFRICAN PERSPECTIVE

Jacobus Young*

Abstract

The use of key risk indicators as a management tool is one of the requirements for the calculation of a bank's operational risk capital charge. This article provides insight into the use of key risk indicators as an operational risk management tool by South African banks and indicates their level of preparedness to comply with the criteria. The results of a questionnaire aimed at junior and middle management indicated that banks are not suitably prepared to implement a key risk indicator management process and have a general lack of understanding of the underlying theory and concept of the criteria to use key risk indicators. The advantages of using key risk indicators are not fully exploited and more benefits can be realised by raising awareness in this regard.

Keywords: Operational Risk, Key Risk Indicators, Quantitative And Qualitative Risk Management Criteria, Risk And Control Self-Assessments, Loss Event Database, Risk Appetite, Risk Thresholds, Early Warning, Risk Reporting

**University of South Africa, PO Box 52185, Wierda Park, Centurion, 0149, South Africa*
Tel.: 012 4293010
Email: youngj@unisa.ac.za

1. Introduction

Nowadays, the management of operational risk by banks is a phenomenon that is widely accepted by most banking industries worldwide. This is substantiated by the fact that most banks are taking cognisance of the qualitative and quantitative criteria for operational risk management advocated by the Basel Committee on Banking Supervision (2003). Although, most banks have accepted these criteria, the criteria are not always implemented effectively. Many global incidents resulting in losses for banks can be related to poor management of operational risk exposures. This phenomenon started long ago and is still a concern. For example, the Barings Bank saga occurred in 1995 during which time a number of the reasons were related to operational risk, such as an inadequate segregation of duties, a lack of effective supervision, awareness and oversight by senior management. A number of recent losses are still linked to these types of exposures, for example, the recent Enron case where senior management was directly involved in fraudulent activities (Davis 2007). Then there is also the recent global financial crisis, which alerted most financial institutions on risk management.

The importance for financial institutions to be able to deal with an economic crisis was confirmed by the G20 Countries' Cannes Summit in November 2011 where it was stated: "*We are committed to improve banks' resilience to financial and economic shocks. Building on progress made to date, we shall call on jurisdictions to meet their commitment to implement fully and consistently the Basel II risk-based framework as well as the Basel II-5 additional requirements on market activities and securitization by end 2011 and the Basel III capital and liquidity standards....*" (Cannes Summit Final Declaration 2011).

According to Jobst (2007), financial globalisation facilitates greater diversity of investment and asset funding across national financial systems. This development seems to foster higher systemic resilience due to more efficient financial intermediation, enhanced allocation of risk and greater asset price competition. As a result, banking regulation and risk management became more complicated and the Basel Committee on Banking Supervision started with reviewing the principles and supervisory regulations governing the capitalisation of internationally active banks (also regarded as systemic banks). These regulatory efforts were mostly aimed at the development of new capital rules in response to greater systematic vulnerabilities from the increasing sophistication of financial products, the diversity of financial institutions and the increasing interdependence of financial markets (Jobst 2007). Included in these endeavours of the Basel Committee on Banking Supervision to address new threats to financial stability, is the approach and management of operational risk. Jobst (2007) states that although operational risk always existed as one of the core risks

of the financial industry, markedly rising geopolitical risk, deficient corporate governance and systemic risk from financial derivatives have the potential to magnify adverse outcomes. These outcomes could result from business activities, inadequate or failed processes and information systems, misconduct by people or from unforeseen external factors.

Concerns about the economic implications of pervasive credit risk transfer across financial institutions and national boundaries in times of systemic crises, lead to efforts to regulate the management of operational risk. Regulators are particularly concerned about incentives that encourage greater risk taking in a benign economic environment but also entail consequences that are more adverse when stress occurs (Jobst 2007).

Banks play an important part in the world economy, which became clear during the recent global financial crisis where a number of banks were liquidated. These typical losses can happen again if banks cease to perform their central role in the economy, and it is therefore imperative that banks maintain their future growth and ensure a sound risk management approach. According to Wellink (2010), banking sectors are at the centre of credit intermediation processes and infrastructures and therefore need to increase their long-term growth. To address the failures revealed by the financial crisis, the Basel Committee on Banking Supervision is introducing fundamental reforms to the international regulatory framework. The reforms strengthen bank-level or micro-prudential, regulations that will help raise the resilience of individual banking institutions through stress periods (Basel Committee on Banking Supervision 2011). According to Henniaux et al (2011), the Basel Committee on Banking Supervision is also introducing a number of macro-prudential elements into the capital framework to assist in containing systemic risks arising from procyclicality and from the interconnectedness of financial institutions. The Committee introduced measures to make banks more resilient towards procyclicality. The primary objectives of these measures are:

- dampen any excess cyclicality of the minimum capital requirements;
- promote more forward looking provisions;
- conserve capital to build buffers at individual banks; and
- achieve the broader macro-prudential goal of protecting the banking sector from periods of excess credit growth (Henniaux et al 2011).

The Basel Committee on Banking Supervision, introduced the capitalisation of internationally active banks since 1999, known as the Basel Capital Accord (Basel I), followed by the New Basel Capital Accord (Basel II) in 2004. Although banks are still in the process of developing and implementing the guidelines of the Basel II Accord, Basel III requires higher capital for systemic banks. According to Henniaux et al (2011), there are many factors that lead to the build up of the financial crisis, but one of the main factors was excess liquidity, which resulted in too much credit and weak underwriting standards causing inadequate liquidity buffers. Although many banks are in an advanced stage of developing and implementing criteria and guidelines based on the Basel II Capital Accord, it is important that banks are aware of their operational risk exposures and that they have ways to mitigate these risks effectively in order not to fall into the trap of making the same mistakes as other institutions.

However, the management of operational risk is not as clear cut as it sounds, because of the difficulty in measuring the risk exposures. The Basel Committee on Banking Supervision (2005) initiated guidelines and criteria on operational risk management, and started by defining operational risk as the risk of losses due to inadequate or failed internal processes, people or systems or external events.

In addition, the Basel Committee on Banking Supervision (2003) identified sound management principles for operational risk. According to one of these principles, banks should implement a process to monitor operational risk profiles and exposures to potentially material losses regularly. There should be regular reporting of pertinent information to senior management and the board of directors. Such information should support the proactive management of operational risk.

The identified qualitative and quantitative criteria to management operational risk require specific tools in order to adhere to these criteria. Key risk indicators (KRIs) can be regarded as such a tool. However, there exists little guidance on the use of KRIs as an operational risk management tool. According to the Institute of Operational Risk (2010), the management of KRIs is an area that has proved to be particularly challenging for many organisations. Ford, Sundmacher, Finch and Carlin (2009) state that, although 40% of financial services firms are in the process of developing and implementing KRIs, there are not much information on the type of KRIs being developed and their effectiveness in managing operational risk. Therefore, it can be concluded that, although organisations are in the process of developing and implementing KRIs, there is still some uncertainty in this regard.

The purpose of this article is to elaborate on the concept of KRIs and to determine the current level of development and implementation by the South African banking industry. The article consists of a literature review and the results of a survey amongst current risk management practitioners in South African banks to determine the current level of development of KRIs as a risk management tool. The results of the survey are used to make recommendations for banks to consider when implementing KRIs to ensure that the maximum

benefits can be achieved during the process of managing the operational risk exposures.

In the next section, the operational risk factors are discussed in order to provide the background and use of key risk indicators as an operational risk management tool into perspective.

2. Operational risk factors

King (2001) states that operational risk measurement deals with risk factors, which are the causal factors that create losses that can negatively influence earnings.

According to the definition of operational risk, there are four causal factors, namely internal people, processes, systems and external events. These factors are applicable for the business and control environment of an organisation, although from an operational risk management perspective, the following risk factors could determine the level of operational risk:

- type of business activity;
- the size of the activity;
- the business environment; and
- the control environment (Ong 2007).

A crucial aspect in the practical use of the operational risk factors is that the identified factors must be measurable in order to ensure that it can determine the level of risk. Ong (2007) states that determining the level of risk is an important point, which must provide detail on what the level of the risk factor is and what must be done about it. Therefore, it is imperative to link a value to the risk factors in order to determine the level of the risk. For example, should a medical doctor identify that a patient is suffering from a heart problem, it is crucial to identify the level of seriousness to understand which remedial steps to take. Should the problem then not be serious, it will not be necessary for a heart transplant. Similarly, it is clear that when managing key risk factors (indicators), the risk factor as well as the level of the risk has to be clearly identified.

Once the risk factors for operational risk are understood and identified, it could be possible to manage key risk indicators (KRIs), but then it is also imperative to understand the concept of KRIs. However, it is also important to understand the origin of the KRIs in terms of the qualitative and quantitative criteria for operational risk management.

3. Operational risk management criteria

According to the Basel Committee on Banking Supervision (2006), a bank must adhere to certain criteria to manage operational risk, which can be divided into qualitative and quantitative criteria, illustrated in Figure 1.

Figure 1. Criteria for operational risk management

Qualitative criteria	Quantitative criteria
1. Independent operational risk management function, responsible for the design and implementation of the operational risk management framework, including policies and procedures, measurement methodology, reporting system and operational risk management process. 2. Operational risk management system that is closely integrated into the daily risk management processes of the bank. 3. Allocation of operational risk capital to major business lines. 4. Incentives to improve the management of operational risk. 5. Regular reporting of operational risk exposures and procedures for taking appropriate action. 6. Documented operational risk management process. 7. Routine for ensuring compliance with internal policies, controls and procedures. 8. Regular reviews of the operational risk management processes and measurement system by internal and external auditors. 9. Validation of the operational risk measurement system by supervisory bodies.	1. Risk measurement system aligned with the loss event types. 2. Regulatory capital calculated as the sum of expected losses and unexpected losses. 3. Measurement system, sufficiently granular to capture the tail losses. 4. Internal data reflecting the business environment and internal control systems. 5. Relevant external data reflecting the business environment and internal control systems. 6. Scenario analysis reflecting the business environment and internal control systems. 7. Credible, transparent and well-documented and verifiable approach for weighting fundamental elements and used to calculate a capital charge for operational risk.

Source: Adapted from the Basel Committee on Banking Supervision 2006

According to the first qualitative criterion, there should be an independent operational risk management function responsible for the design and implementation of the operational risk management framework, including policies and procedures, measurement methodology, reporting system and operational risk management process. The 4th and 5th quantitative criteria stipulate the use of internal data, relevant external data and internal control systems and the business environment. These criteria indicate that an institution's operational risk measurement system should have four key elements: internal data, external data, scenario analysis, and factors reflecting the business environment and internal control system.

Similarly, it is important to incorporate all four key elements into an operational risk management process. Internal data provide information on institution-specific loss types, while external data provide information on any loss types for which internal data are not available. The business environment and internal control factors (which can be regarded as KRIs) provide information on how risk is mitigated or magnified by qualitative environmental factors. Exactly how the four elements are combined (i.e. the weighting of the four elements) is up to the institution.

To comply with the criteria for operational risk, most banks make use of the following methods to identify and assess operational risk:

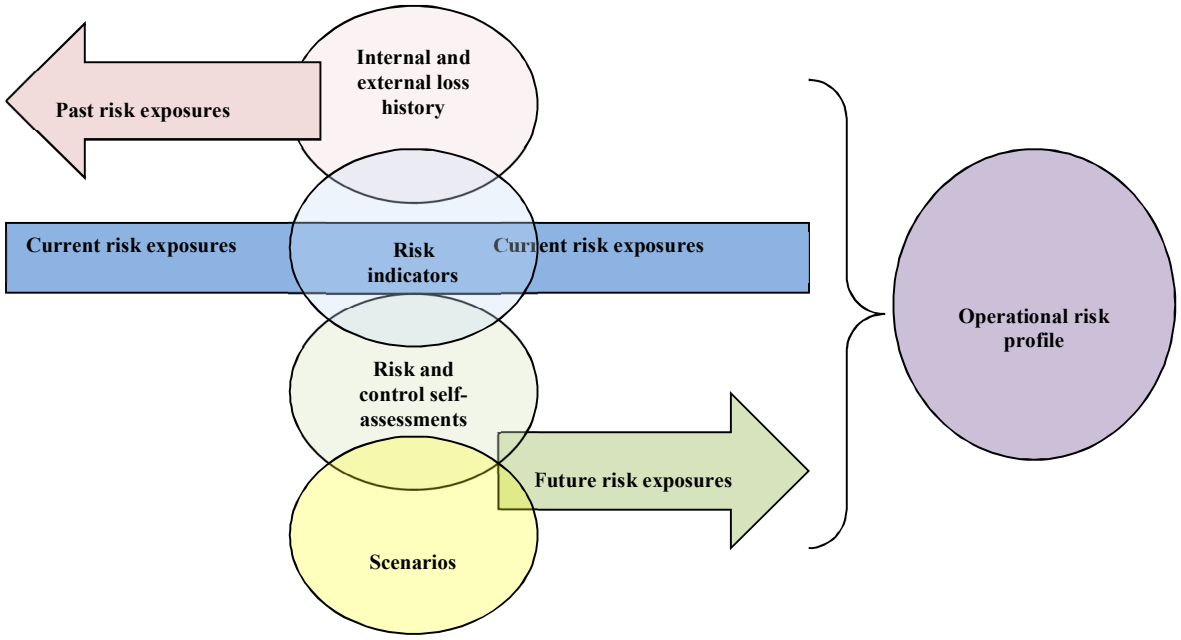
- The loss event database. The analysis of historic losses that a bank experience could provide meaningful information for assessing the bank's exposure to operational risk and for developing a policy to mitigate/control the risk exposure. An effective way of making use of this information is to establish a framework for systematically tracking and recording the frequency, severity and other relevant information on individual loss events. Some firms have also combined internal loss data with external loss data, scenario analysis and risk assessment factors in order to ensure a more objective analysis of the loss data (Basel Committee on Banking Supervision 2003).
- Key risk indicators. This method refers to statistical information, which could provide insight into a bank's risk position. These indicators tend to be reviewed on a periodic basis to serve as an early warning system for banks to initiate proactive control or preventative measures for risk exposures. The frequency of reviewing and reporting on KRIs depends on the importance of the indicator, which is determined by management.
- Risk and control self-assessments. This method is used to assess a bank's operations and activities against a menu of potential operational risk exposures and vulnerabilities. The process is internally driven and often incorporates the use of scorecards, which will translate qualitative assessments into quantitative metrics. However, the use of these scores can be very subjective and should therefore be tested by means of additional assessments. King (2001) states that risk and control self-assessments are used to identify important risks to an organisation whereby responsible parties are requested to subjectively assess various parts of the organisation and its characteristics. According to Ford et al. (2009), KRIs, augmented by risk and control self-assessments, would help inform a better forecast of future losses from operational risk and foster a more accurate allocation of regulatory capital.
- Scenarios. During a process of scenario analysis, it is expected of internal experts to give their views on the applicability of identified operational risk factors. According to Kalyvas and Akkizidis (2006), scenario analysis is a methodical way of getting professional opinions from business and risk managers to gain rational evaluation of the probability and impact of probable operational losses. This can be achieved, for example, by verifying the likelihood and potential impact of KRIs.

In general, it is accepted that the above methods can be used to identify the history of the losses, the current view of risk exposures and the future potential risks. This is reflected in Figure 2.

The figure illustrates the four primary tools to determine risk exposures. The internal and external loss history can be used to identify risk exposures, which the organisation had experienced in the past. Risk and control self-assessments and scenarios are used to identify potential future risk exposures and the KRIs can be used to identify the current risk exposures for the organisation.

Kalyvas and Akkizidis (2006) state that operational risk identification can be based on the operational KRIs, and KRIs are becoming increasingly important tools in the framework of operational risk management systems. It is apparent that KRIs are used to determine the current operational risk exposures and to serve as early warning. This is elaborated on in the next section.

Figure 2. The use of operational risk methods



Source: Author's own interpretation

The figure illustrates the four primary tools to determine risk exposures. The internal and external loss history can be used to identify risk exposures, which the organisation had experienced in the past. Risk and control self-assessments and scenarios are used to identify potential future risk exposures and the KRIs can be used to identify the current risk exposures for the organisation.

Kalyvas and Akkizidis (2006) state that operational risk identification can be based on the operational KRIs, and KRIs are becoming increasingly important tools in the framework of operational risk management systems. It is apparent that KRIs are used to determine the current operational risk exposures and to serve as early warning. This is elaborated on in the next section.

4. Concept of key risk indicators

Key risk indicators can be regarded as metrics that can be used to monitor the identified risk factors over time. However, it is important to note that an indicator becomes *key* when it tracks a risk exposure, which could have a major influence on the organisation. According to the Institute of Operational Risk (2010), an operational risk indicator is a metric that provides information on the level of exposure to a given operational risk that the organisation is experiencing at any time.

Alexander (2003) defines KRIs as statistics and/or metrics, often financial, which can provide insight into a bank's risk position. These indicators tend to be reviewed on a periodic basis to alert banks to changes that may be indicative of risk concerns. Such indicators may include the number of unsuccessful and failed trades, staff turnover rates and the frequency and/or severity of errors and omissions.

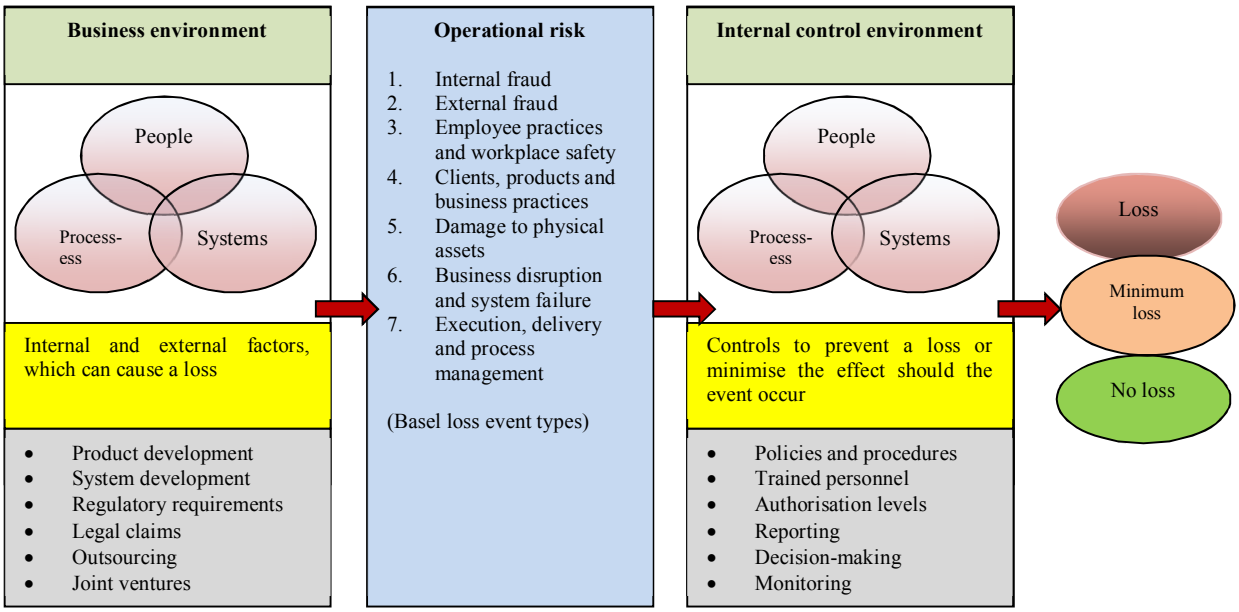
According to Kalyvas and Akkizidiz (2006), KRIs are mathematical functions that include all those parameters that describe the operational variation of specific operations within specific business lines. Young (2006) states that KRIs are mostly quantitative measures intended to provide insight into operational risk exposures and control measures.

Using KRIs is one way of measuring the actual value of the cause and the consequence of a risk event (Kalyvas and Akkizidiz 2006). The benefit in managing KRIs lies in the provision of predictive information to facilitate decision-making and enable preventative actions. Ong (2007) argues that KRIs are used to indicate operational risks or a change in the operational risk profile. These KRIs should be formulated specifically for individual activities or value chain processes if they are to be significant, since different processes may require different indicators. Even the same indicators may require different interpretations in certain circumstances, such as different warning thresholds. According to Ong (2007), an analysis of a particular activity or process will reveal whether the organisation's past development is consistent with the scenario assessments for the activity or process.

As such, it is important that KRIs be managed by means of a quantitative approach. Figure 3

illustrates the concept of KRIs for operational risk management further.

Figure 3. Key risk indicators for operational risk



Source: Adapted from Ong 2007

The figure shows the three primary risk factors for operational risk and typical internal and external factors that could influence the organisation's risk exposures. Examples are product and system developments, outsourcing and regulatory requirements. According to the Basel Committee on Banking Supervision (2001), a bank should categorise operational losses into seven loss event types, which are intended to group operational risk losses into distinct components according to the nature of the underlying operational risk event. The aim is eventually to arrive at a comprehensive assessment of the true operational risk profile within and across institutions. The last phase involves the control environment, where controls are developed and implemented to prevent losses or to minimise the loss should a risk event occur.

Davis (2007) states that KRIs sounds like a straightforward concept, measuring and reporting the items that may give cause for concern; however, there are many challenges associated with the concept, for example:

- is the right thing being measured?
- are the measures accurate?
- are the definitions clear?
- are truly key risk indicators identified?
- how are the KRIs depicted? and
- can the KRIs be used to determine the current risk exposures?

According to Hoffman (2002), operational risks will not be effectively identified without first identifying the key risk indicators of operational risk. The main challenge in dealing with operational risk indicators is in identifying or constructing metrics that serve as predictors of operational risk.

During the identification of the quantifying parameters of the risk indicators, the following aspects should be considered:

- the actual degree of severity, size of intensity that describes the observed extent of the presence of operational risk;
- the frequency of risk existence and measuring their parameters – the frequency describes the number of times a risk of a given size occurs within a given period of time;
- the context-dependency relation, which may differ in certain situations; and
- the possible correlation and its sign with other indicators based on the common parameters among all indicators (Kalyvas and Akkizidiz 2006).

In addition, KRIs should have the following characteristics in order to be used as a tool to management operational risk:

- the data must be available;
- the data must be quantifiable in either percentage, value or volume;
- a tolerance threshold must be determined by management and must only change according to changing circumstances, and
- the KRIs must be monitored on a regular basis.

The Institute of Operational risk (2010) furthermore states that indicators must be capable of being measured with a high level of certainty and on a

repeated basis. Therefore, indicators should be numbers/counts, monetary value, percentages, ratios, time duration or a value of some pre-defined rating set. A very important aspect is that, when an indicator is identified, the measurement is agreed to by all stakeholders to ensure that everyone agrees what the value represents, how it is calculated, what is included or excluded and how variances in the values will be dealt with (Institute of Operational Risk 2010).

From the above discussion, it can be concluded that KRIs play an important role in the management of operational risks, although it is not always possible to determine a universal set of KRIs for any given organisation. However, to ensure that KRIs add value during the operational risk management process, it is imperative to consider and provide answers to the above questions, considering the purpose of KRIs to provide guidelines in answering these questions.

5. Purpose of key risk indicators

KRIs can be used in managing operational risk in a number of ways, for example:

- Early warning. KRIs can be used to serve as an early warning mechanism for risks that are imminent, which will allow management to take preventative actions. According to the Institute of Operational Risk (2010), KRIs, if selected appropriately, can provide a means of identifying:
  - emerging risk trends;
  - current exposure levels; and
  - events that may have materialised in the past and which could re-occur.
- Support risk assessments. Indicators can be used to support risk assessments by indicating whether pre-assigned thresholds or limits are breached, and require the development and implementation of control measures.
- Determine a realistic risk appetite. KRIs can add value in the sense that it can serve as an input to determine a realistic risk appetite. The Institute of Operational Risk (2010) states that an organisation is able to see whether its operational risk exposures remain within its appetite for risk or exceed it. Hence, the monitoring of KRIs is an important mechanism by which an organisation's management can gain assurance that it remains within its stated appetite for operational risk.
- Capital allocation. KRIs can be used as a supporting tool to calculate an accurate capital allocation for operational risk. The Institute of Operational Risk (2010) states that, in terms of regulatory sound practice principles, it is generally accepted that every organisation needs a mechanism to measure and monitor its current levels of operational risk exposure, a process that KRIs can support. Furthermore, KRIs are regarded as complying with the following criteria in order to calculate a regulatory and economic capital for operational risk:
  - it is risk-sensitive;
  - it provides management information on the risk profile;
  - it represents meaningful drivers of exposure which can be quantified; and
  - it can be used across the entire organisation (Institute of Operational Risk 2010).

The Institute of Operational Risk (2010) concludes that the KRIs are the most appropriate mechanism to satisfy the regulatory requirements, implying that there is an indirect regulatory requirement to implement and maintain an active KRI programme.

To use KRIs as an operational risk management tool, it is necessary to develop a process to determine the KRIs, who should represent reporting parameters for performance benchmarking and early warning signal generation that will serve as integrated part of an optimal risk monitoring system.

6. Key risk indicator process

According to Davis (2007), the risk appetite and tolerance of the organisation are embedded into the risk management process via the KRIs. The levels of KRI thresholds or tolerance are an indication and quantification of the organisation's risk appetite. In this sense, what is required to determine the threshold in the design of the KRIs, is the initial collation and aggregation of the required data based on an appropriate data model.

The process of managing KRIs can be divided into two parts. The first part is to identify the KRIs and the governance issues. This can be done by means of the following steps:

- Identify and analyse a business process (process flow analysis).
- Perform a risk and control self-assessment of the business process to identify the inherent risk, control measures and residual risks of the business process.
- Prioritise the residual risks in terms of high, medium and low risks.
- Identify the indicators according to the characteristics of a KRI:
  - the risk must be a high priority (high risk);
  - the KRI must be quantifiable; and
  - the data must be available.
- All stakeholders agree to a threshold for the KRIs.
- Register the indicator as a KRI.
- Determine the roles and responsibilities in managing the KRIs.
- Determine the reporting frequency and method, including escalation and reaction procedures should the report indicate a breach in the predetermined threshold.

- Determine the application of the KRIs as an input to calculate a capital charge for operational risk.

The second part is the actual managing of the KRIs according to the approved governance procedures, which could include the following steps:

- Collate the data required at the approved times.
- Draft the report according to the approved format.
- Submit the report according to the approved timeframes and to the approved role players.
- Develop and implement control measures if there is a breach in the approved threshold.
- Monitor the various business influences, which could lead to a change in the approved threshold, for example an increase in business, external influences on business processes, etc.
- Submit KRI information to serve as an input for operational risk modelling (to determine a realistic capital for operational risk).
- Submit KRI information as an input to determine the operational risk profile and the risk appetite of the organisation.
- Submit KRI information to test the risk and control self-assessment results.

In order to embed a process to manage KRIs, it is imperative that an organisation must have an approved policy for managing KRIs. This policy should include the abovementioned steps and specifically the governance issues that will indicate the various roles and responsibilities of all stakeholders.

Although there might be many more uses and methods to manage KRIs as an operational risk management tool, the above steps could serve as a guideline for implementation. However, to have a clear and streamlined KRI management process is critical in establishing a healthy approach to operational risk management throughout the business environment. Therefore, being aware of threats in advance and being able to predict and manage the risk exposures is essential to ensure the successful continuation of the business.

The empirical research of this article was based on the aforementioned literature review on KRIs, to serve as a platform to develop a suitable research methodology that is discussed in the ensuing section.

7. Research methodology

In order to determine the current level of development and implementation of KRIs by banks as well as the knowledge base of employees to use KRIs with the aim to manage operational risk, a questionnaire was used to collect information. The target group was identified as junior and middle managers from the banking industry in South Africa. The respondents mostly consisted of risk managers and business managers who represented the important role players involved in managing a bank's operational risks. The reason for using this target group was that it is usually at this level where processes and systems are physically implemented and where the success of new implementations is determined. Therefore, the response can be accepted as a reasonable reflection of the status of the use of KRIs by the banking industry.

The aim of the questionnaire was to determine whether the banking industry in South Africa is using the concept of KRIs as an operational risk management tool and to determine the level of implementation and knowledge of employees who are involved in this process.

The questionnaire requested respondents to indicate on a 6-point Likert scale their views and experiences regarding specific questions on the concept of KRIs and the level of implementation by their bank. The response was analysed in terms of descriptive statistics according to the following scale:

1. To a full degree
2. To a degree
3. To a moderate degree
4. To some degree
5. To no degree
6. Do not know

In the rare case of a respondent not selecting one of the six options, it was assumed that he or she did not understand the issue.

8. Research results

The questionnaire was distributed to a population of 60 junior and middle managers of various banks in the South African banking industry. Thirty-one questionnaires were returned on the due date, which represented a 52% response rate.

The formulated questionnaire consisted out of 25 demographic and subject-related questions. The aim of the demographic questions was mainly to determine the involvement of the respondent as well as his/her experience in risk management. According to the response, 64% indicated that they were involved in the bank's risk management from an operations perspective, while 27% was in the banking insurance section and 9% in other sections of a bank. From an experience perspective, 9% of the respondents had been employed for less than one year, 27% between 1 and 3 years, 9% between 3 and 5 years, 19% worked at their company between 5 and 10 years, and 36% had been with their employees for more than fifteen years. As such, it can be concluded that the response to the questionnaire could be accepted as valid in terms of the roles of the respondents, involvement in risk management (64% were involved in risk management) and average years of experience in a banking environment (55% had been working at a bank for more than 5 years).

The response on the questionnaire is divided into the following categories:

- Understanding key risk indicators as a risk management tool.

- Application of key risk indicators within the organisation.
- Policy and reporting.

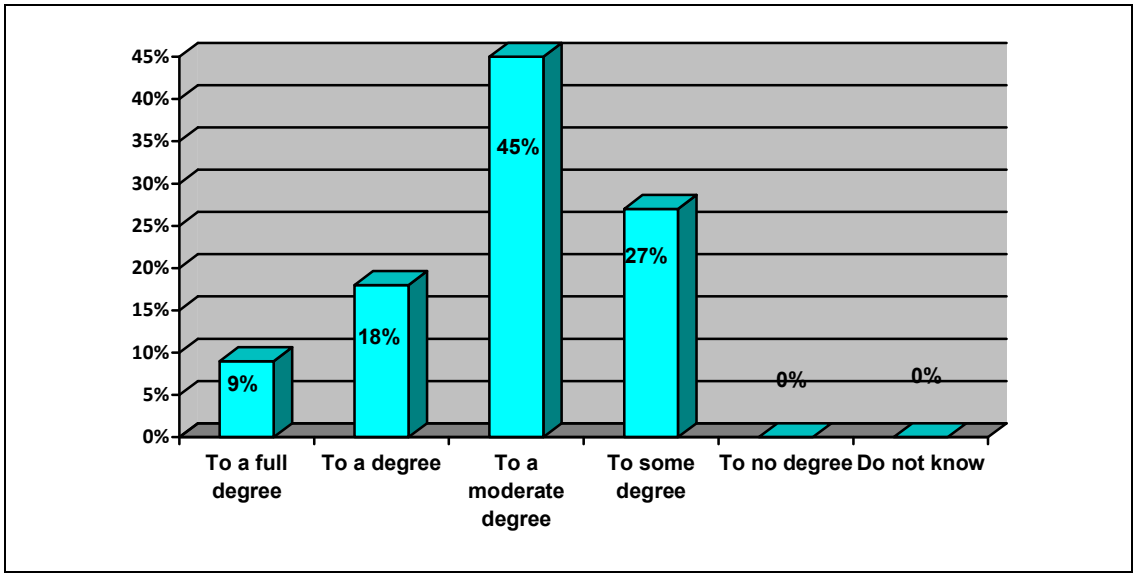
The categories are discussed in the next section in terms of the results of the survey.

8.1 Understanding of key risk indicators as a risk management tool

Fifty-one per cent of the respondents indicated that they understand the concept of risk indicators as a risk management tool to a full degree, while 49% understood it to a degree. As such, it can be concluded that there is a strong indication that all respondents understand the concept of KRIs as a risk management tool.

More than 70% of the respondents deemed KRIs to be moderately to fully defined as a risk management tool by their organisation (Refer to Figure 4). This showed that employees should understand KRIs and know how to use it as a risk management tool.

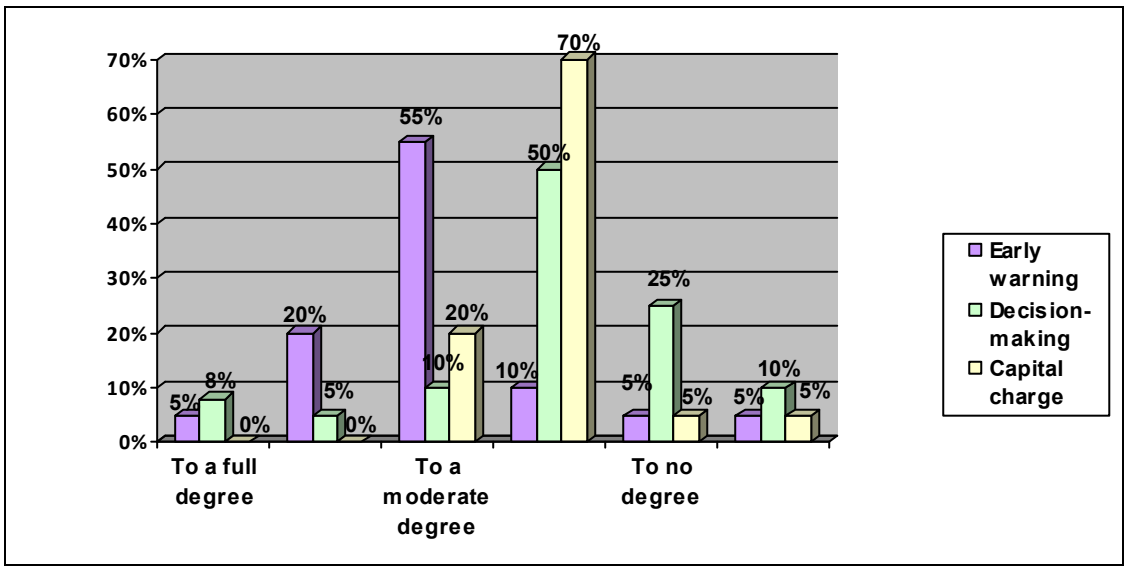
Figure 4. Understanding of key risk indicators as a risk management tool



Although the concept of KRIs is broadly understood and defined by most organisations, the question is to what extent it is being applied by the organisation.

The benefits of implementing a successful KRI management process could ensure that it can serve as an early warning indicator, a basis for proactive decision-making and to assist in the calculation of a realistic capital charge for operational risk. Figure 5 indicates the responses from the respondents on the abovementioned.

Figure 5. Potential benefits of a key risk indicators management process



According to the responses, 55% of the respondents indicated that KRIs serve as early warning indicators to a moderate degree, clearly showing a lack of the effective use of the methodology as a risk management tool. As such, it can be concluded that the use of KRIs is still at grass-roots level in the banking environment and not being exploited to the maximum as a risk management tool.

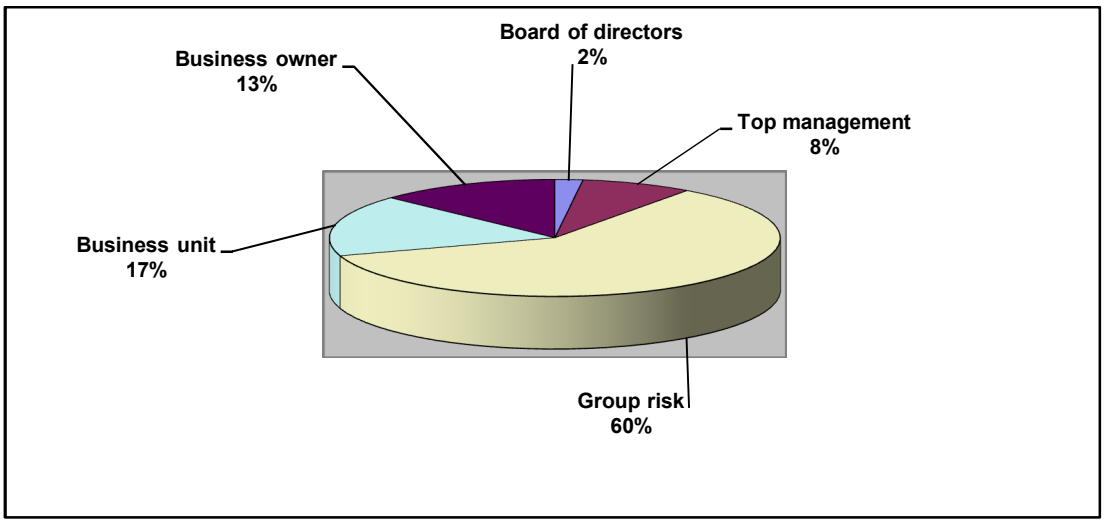
Evidence (see Figure 5) also indicates that KRIs are being used to some degree (50%) as a decision-making tool. This is another indication that KRIs are not being used to their fullest extent when it comes to assisting management in making decisions. Of the respondents, 8% and 20% indicated that KRIs are being used to a full degree and to a degree for decision-making respectively. Therefore, it is clear that there is a definite movement in the right direction to use KRIs for decision-making; however, the large percentage (50%) that indicated the use only to some degree, illustrates that there is still much room for improvement.

The application of KRIs to assist in the calculation of a capital charge for operational risk is clearly not adequate, because the majority of the respondents indicated that KRIs are not being used to calculate a realistic capital charge for operational risk. Eighty per cent of the respondents indicated that KRIs are being used to some degree; however, this response reflects a clear shortfall of the effective use of KRIs (Refer to Figure 5).

8.2 Application of key risk indicators within the organisation

The respondents indicated that KRIs are mostly being used at a group risk level (60%), 30% at a business unit and risk owner's level, and 10% at top management level (Refer to Figure 6).

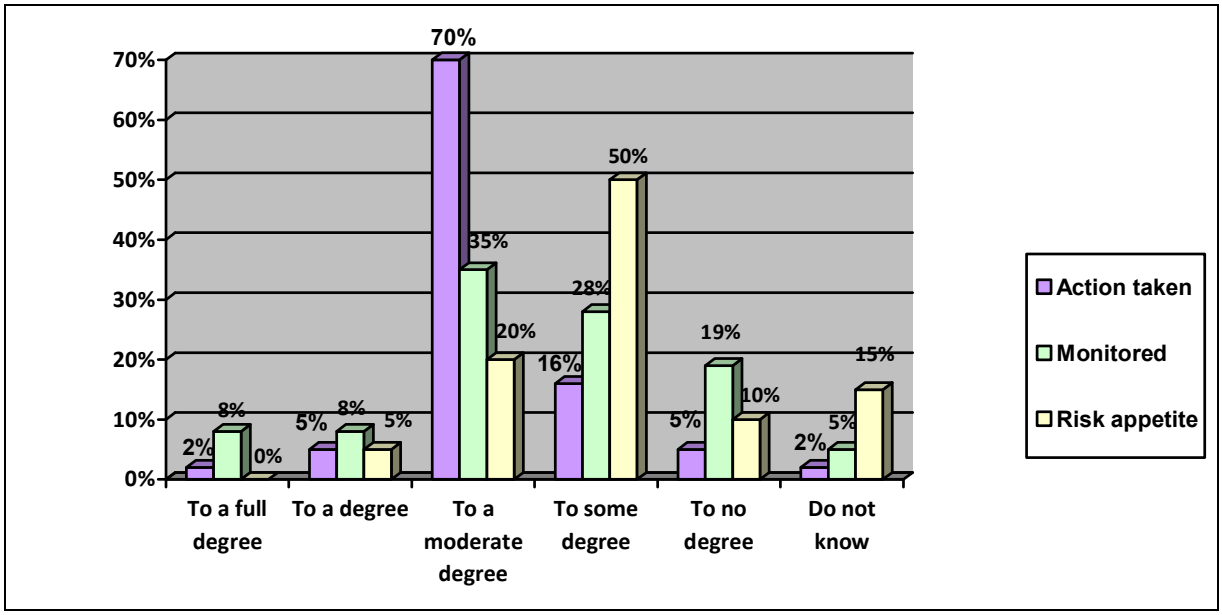
Figure 6. Use of key risk indicators at management levels



Usually, risk management tools are developed by the risk management department before being implemented throughout the organisation. As such, it seems that, in general, the use of KRIs could still be in a development stage and being either tested or rolled out from a centralised (group risk) level. KRIs is a bottom-up approach to risk management and should, therefore, be used mostly at business unit and risk owner levels.

Evidence (see Figure 7) show that the responsibility to manage KRIs is usually delegated to a responsible manager. Of the respondents, 15%–25% indicated that the responsibility is delegated to a full degree or to a degree to a responsible manager respectively, while 50% indicated that it is delegated to a moderate degree. However, the actual management of the KRIs is not always adequate, taken into account the response on the action taken where the threshold is breached. As illustrated in Figure 7, 70% of the respondents indicated that preventative and corrective action is taken to a moderate degree when the threshold of a KRI is breached.

Figure 7. Action taken when a key risk indicator threshold is breached



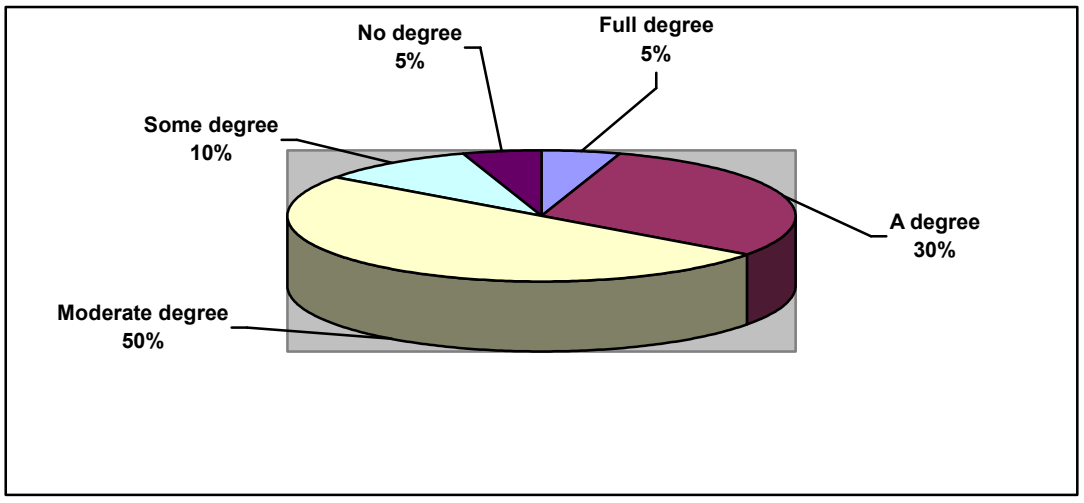
It can be concluded that KRIs are still being managed at a level where it does not provide adequate information for management to make corrective or preventative decisions. As such, it seems that KRIs are mostly still in a developmental phase and not being used adequately as a risk management tool. In addition, the responses also indicated that changes to KRI scores are monitored from a moderate (35%) to some (28%) degree, which could imply that the use of KRIs is still at a very average implementation level. This conclusion can also be supported by the response on the use of KRIs to determine the risk appetite of the organisation. Twenty per cent of the respondents indicated that KRIs are being used to a moderate degree and 50% indicated to some degree. The majority of the respondents (75%) who indicated to some degree, to no degree and do not know, believe that the KRIs are not being used as a management tool to determine the organisation's risk appetite.

Another important issue with the management of KRIs is the policy regarding the implementation of the KRI process and the reporting frequency.

8.3 Policy and reporting

It is imperative that the KRI management process be incorporated into an organisational policy. According to the respondents, 5% and 30% indicated that the KRI management methodology is incorporated into a formally approved policy to a full degree and to a degree, respectively. Fifty per cent indicated that a KRI management policy is in existence to a moderate degree (Refer to Figure 8).

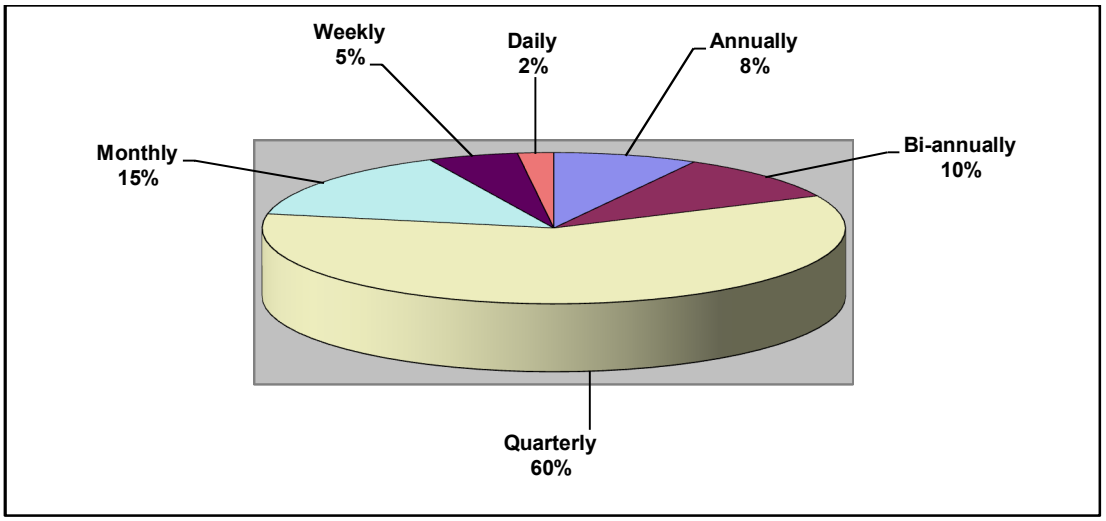
Figure 8. Degree that key risk indicator methodology is incorporated into a formally approved policy



It can be deduced form the abovementioned response that most banks do have a formal policy for the management of KRIs. However, the majority of the response (50%) indicated that this is only to a moderate degree. As such, it can be concluded that, although there do exist formal policies for the management of KRIs, it must yet be promulgated throughout the organisation.

The success of managing KRIs is also dependent on the adequacy and frequency of reporting. Figure 9 indicates the response on the frequency of reporting on KRIs.

Figure 9. Frequency of reporting on key risk indicators



Sixty per cent of the respondents indicated that KRIs are being reported quarterly, while 5% and 2% indicated weekly and daily respectively. The success of managing KRIs lies within the adequacy and the frequency of reporting and the subsequent action to be taken. According to the response, the reporting of KRIs is mostly done on a quarterly basis. This could indicate that the use of KRIs is not at an acceptable level according to the methodology and potential benefits, which could be acquired from an adequate KRI management process. Therefore, it confirms that the use of KRIs is still in its initial phases of development and implementation.

9. Conclusion

Although operational risk management should by now be an embedded part of a bank's management processes, there are still uncertainties surrounding the application of the various management tools. These tools must be used to adhere to the qualitative and quantitative criteria to manage operational risk exposures. KRIs comprise one of these tools. Although most banks are using KRIs as a risk management tool, there seems to be some uncertainty with its application. This article aimed to elaborate on the concept of KRIs and to determine the current level of implementation by the South African banking industry.

Before KRIs can be used as an operational risk management tool, it is imperative to understand the underlying concepts, such as the risk factors that were identified as people, processes, systems and external events. The use of KRIs is also supported by the criteria for operational risk management that were identified by the Basel Committee on Banking Supervision. To comply with these criteria, most banks use the following management tools:

- a loss event database;
- key risk indicators;
- risk and control self-assessments; and
- scenarios.

KRIs are regarded as metrics that can be used to monitor the identified risk factors over time. KRIs provide management with current management information in terms of the organisation's risks. Therefore, KRIs should have certain characteristics before they can be used as a risk management tool, for example:

- data must be available;
- data must be quantifiable;
- a tolerance threshold must be determined; and
- KRIs must be monitored on a regular basis.

Once these characteristics are present, there are many benefits which can be exploited in using KRIs as a risk management tool, such as:

- serving as early warning to management to take corrective or preventative control actions;
- supporting risk and control self-assessment processes to identify risk exposures;
- adding value when determining the risk appetite; and
- supporting the process to calculate a realistic capital allocation for operational risk.

It is furthermore crucial that KRIs be managed according to a formal management process that should be incorporated in an approved policy. The

policy should also clearly indicate the roles and responsibilities of various role players to ensure successful application of the KRI process.

The response to the survey questionnaire provided some insight into the level of implementation of KRIs as an operational risk management tool and the current knowledge of employees in South African banks. The questionnaire was constructed in such a way that it allowed conclusions in terms of the following categories:

- understanding KRIs as a risk management tool;
- application of KRIs within the organisation; and
- policy and reporting.

According to the results of the empirical analysis, the following main conclusions are made:

- banks seem to understand the use of KRIs as an operational risk management tool;
- although KRIs are being used to a moderate degree by most of the participating banks, they are still in the initial implementation phase;
- junior and middle managers seem to be knowledgeable about the concept of KRIs, but apparently, there is a lack of knowledge regarding the implementation thereof at a lower management level;
- banks appear not to be fully aware of the value and benefits that the successful implementation of a KRI management process could ensure;
- evidence illustrated that KRIs are not effectively used as early warning indicators to management to make proactive and corrective risk control decisions;
- it seems as if the banks are aware of the value of KRIs during a decision-making process, but this benefit is currently not fully exploited;
- apparently, the use of KRIs is not successfully supporting the calculation of a capital charge for operational risk;
- it seems as if most banks are conducting the use of KRIs at a group risk management level. This could be an indication that the methodology of KRIs is still being developed and tested before it is rolled out to a risk owner level;
- it can also be concluded that, although the management of KRIs is delegated to a responsible manager, the actual management of the actions required when a threshold of a KRI is breached is still not adequate;
- evidence shows that the use of KRIs to assist in determining the risk appetite is inadequate;
- although it is evident that most banks do have a formally approved policy for KRI management, it seems that such policy must still be promulgated and embedded throughout the organisation; and
- it is evident that the frequency of reporting on KRIs is inadequate. It was indicated that most KRI reporting is only quarterly, which is in contrast with the reporting requirements of KRIs.

The following recommendations can be useful for banks to consider when developing and implementing a KRI management process as an operational risk management tool:

- before implementing a KRI management process, it is imperative to embed the process throughout the organisation by means of training sessions, awareness campaigns and the launching of pilot studies. During this process, it is important that all role-players be made aware of the policy requirements as well as the objectives of KRIs, for example:
  - to serve as an early warning indicator for proactive preventive or corrective control measures;
  - to add value during the calculation of the capital charge for operational risk;
  - to add value during the defining of the risk appetite; and
  - to provide data for reporting purposes to top management and regulatory purposes.
- new employees should be trained to ensure that KRIs are being managed continuously; and
- reporting on KRIs should be done at least monthly to ensure adequate actions when a threshold is breached. If only quarterly reporting is required, it can be assumed that the indicator is not a KEY indicator, but a normal indicator, which requires a lower level of monitoring.

The analysis was restricted to and based on a limited number of junior and middle managers of certain South African banks. Consequently, any generalised deductions and conclusions cannot be made applicable to the whole South African banking industry. Therefore, it is recommended that this article be used as a guideline for more detailed research regarding the various practical aspects of the development and implementation of a KRI management process.

Notwithstanding the limitations of this article, it is crucial that banks ensure that a sound KRI management process is embedded to serve as an operational risk management tool and that all employees are knowledgeable and therefore prepared to exploit the benefits of a KRI management process for the organisation.

References

1. Alexander, C. 2003. Operational Risk: Regulation, Analysis and Management. Pearson Education Ltd, London.
2. Basel Committee on Banking Supervision. (2001). Working Paper on the Regulatory Treatment of Operational Risk. September 2001) p.3. Bank for International Settlements.
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. 2005. The Joint Forum- High-level principles for business continuity. [Online] Available from \http://www.bis.org/publ/joint14.pdf. [Accessed: 2011-02-10].
5. Basel Committee on Banking Supervision. (2006). International Convergence of Capital Measurement and Capital Standards. A Revised Framework. Comprehensive Version: June 2006.
6. Basel Committee on Banking Supervision. 2011. Basel III: A global regulatory framework for more resilient banks and banking systems, Bank for International Settlements, Basel, Switzerland.
7. Cannes Summit Final Declaration G20 Countries. 4 November 2011. Building our Common Future: Renewed Collective Action For The Benefit of All
8. Davis, E. 2007. Operational Risks 2.0. Driving Value Creation in Post-Basel II Era. Risk Books, Incisive Financial Publishing Ltd. London.
9. Ford G. Sundmacher M. Finch N. and Carlin T. (2009). Operational Risk Disclosure in Financial Services Firms in Operational Risk toward Basel III. Best Practices and Issues in Modelling, Management, and Regulation. Edited by Gregoriou, GN. John Wiley & Sons, Inc, New Jersey.
10. Henniaux, E., Adas, R., Wampach, C., Marcy, P., Pierre, G., Borgognoni, P., Ludovicy, C. & Lopez, T. 2011, "Basel III: A risk management perspective - 2011", Basel III recent developments PWC, Luxembourg, 25 May 2011.
11. Hoffman D.G. 2002. Managing operational risk: 20 firm wide best practice strategies. Chicago, USA: Wiley.
12. Institute of Operational Risk. 2010. Operational Risk Sound Practice Guidance: Key Risk Indicators. Institute of Operational Risk, November 2010.
13. Jobst, A.A. 2007. The treatment of operational risk under the New Basel framework: Critical issues. Journal of Banking Regulation. Volume 8, 4 p. 316 – 352. Palgrave Macmiillan Ltd.
14. Kalyvas, L and Akkizidis, I. 2006. Integrating Market, Credit and Operational Risk: A complete guide for bankers and risk professionals. Published by Risk Books Incisive Financial Publishing Ltd. London.
15. King, J.L. 2001. Operational Risk: Measurement and Modelling. John Wiley & Sons Ltd. West Sussex, England.
16. Ong, M. 2007. The Basel Handbook: A guide for financial practitioners. 2nd Edition. Published by Risk Books Incisive Financial Publishing Ltd. London.
17. Wellink, N. 2010. Fundamentally strengthening the regulatory framework for banks. BIS Review, 112: 1-5. [Online] Available from: http://www.bis.org/speeches/sp100903a.pdf. [Accessed: 2011-02-16].
18. Young, J. 2006. Operational Risk Management: The practical application of a qualitative approach. Van Schaik Publishers. Pretoria.