Journal of Financial Risk Management, 2015, 4, 187-205
Published Online September 2015 in SciRes. http://www.scirp.org/journal/jfrm
http://dx.doi.org/10.4236/jfrm.2015.43015

Proposal for an Implementation Methodology of Key Risk Indicators System: Case of Investment Management Process in Moroccan Asset Management Company

Hajar Mouatassim[1], Abdelmajid Ibenrissoul[2]

[1]Doctoral Studies Center—Management, Financial System and Risk Management Laboratory, University Hassan II, Casablanca, Morocco
[2]Doctoral Studies Center—Management, Innovation and Economy Laboratory, National School for Commerce and Management (ENCG), University Hassan II, Casablanca, Morocco
Email: mouatassim.hajar@gmail.com, a-ibenrissoul@hotmail.fr

Received 30 August 2015; accepted 27 September 2015; published 30 September 2015

Abstract

Operational risk is a prominent preoccupation of all managers these days. Indeed, the development of collective awareness has led executives to implement a wide variety of solutions in order to keep this risk and its consequences under control. In this context, we propose a practical implementation methodology of key risk indicators system with the aim to identify operational risks and above all to propose preventive and corrective measures capable of monitoring and managing operational risks. The proposed system will be adjusted to Investment Management process in a Moroccan Asset Management Company.

Keywords

KRI, Operational Risk, Risk Mapping, Standardization Process, Investment Management

1. Introduction

Nowadays, operational risk management has become a priority for all managers. Indeed, with the latest wave of accounting and corporate scandals that have affected the major economic players, reference is made to the

How to cite this paper: Mouatassim, H. and Ibenrissoul, A. (2015). Proposal for an Implementation Methodology of Key Risk Indicators System: Case of Investment Management Process in Moroccan Asset Management Company. *Journal of Financial Risk Management, 4,* 187-205. http://dx.doi.org/10.4236/jfrm.2015.43015

structural reforms of the corporate governance system. At the national level, the sell-off of many insurance companies in the 1990's, the fraud scandals in pension funds and banks in the previous decades have put operational dysfunctions in the spotlight.

All these events have contributed significantly to increase both regulator and executives' awareness. Consequently, regulatory systems have become more stringent and greater importance has been placed on corporate governance, transparency and ethics issues since then.

With regard to regulation, many legislation and standards have been enacted (Sarbanes-Oxley law in US[1], Financial security law in France (FSL), Basle II and III, Solvency II, etc.) in order to strengthen internal control and risk management, especially in listed enterprises, financial institutions and insurance companies. The main objective is to reduce the impact of risks that compromise the achievement of strategic and operational goals and sometimes threaten even the enterprise sustainability.

Key risk indicators have proven to be powerful tools for identifying risk events that impair the smooth running of activities and the achievement of enterprise goals. These indicators are in fact measures that help to follow operational risk exposure in detail. Furthermore, the enterprise can dynamically manage and prevent risks by identifying areas of risk at the earliest possible stage and then take the necessary measures to avoid or reduce potential losses. In the moroccan context, major public and private institutions are looking for powerful tool to deal with operational risk. However, they remain at the theoretical stage concerning key risk indicator system, which is relatively new device compared to risk mapping or scenario analysis tools.

Therefore, we focus on this work on three main issues:

- Analyzing normative framework in regard to setting up key risk indicators and highlighting its limitations;
- Proposing a solution for operational key risk indicators system's implementation in Investment Management process, which consists essentially on identifying upstream difficulties and proposing ways to overcoming them;
- Introducing a systematic and practical approach to meet the challenges.

This work will be undertaken in two parts. The first one will focus on enterprise operational risks and steps to setting up the key risk indicators system. The second part will be dedicated to the process of implementing the proposed tool.

2. Enterprise Operational Risks: From Definition to Setting up Means to Manage Them

Operational risk issue has become a major challenge for all the market players especially after the outbreak of financial scandals during the last years. In fact, their consequences (huge financial losses, bankruptcies, etc.) left no one indifferent. It is from this perspective that regulators and market authorities have tried to better understand this notion. Their common goal is to prevent or limit the negative effects of such risks.

First, we need to define enterprise operational risk and then to detail the means used to limit its negative impact. We will propose finally an implementation approach of key risk indicators system.

2.1. Enterprise Operational Risk

2.1.1. Definition of Operational Risk

Operational risk is one of the most widespread risks and the most significant one faced by firms, since this kind of risk includes a wide variety of hazards. In fact, many researchers, institutions and major banks have tried to converge to universal definition but it has taken different forms overtime.

Some banks, including the BIS[2], have defined first the operational risk as "any risk not categorized as market or credit risk" or as "the risk of loss arising from various types of human or technical error" and many banks "associate operational risk with settlement or payments risk and business interruption, administrative and legal risks" (BCBS[3], 1998).

The definition of the BBA[4] (1999) that was taken up by the Basel Committee (2001) [CD] and which assumes

[1]Sarbanes-Oxley Act was passed by U.S. Congress (2002) to protect investors from the possibility of fraudulent accounting activities by corporations. SOX mandated strict reforms to improve financial disclosures from corporations and prevent accounting fraud.

[2]Bank for International Settlements.

[3]Basel Committee on Banking Supervision.

[4]British Bankers Association.

that operational risk is "the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events", was largely criticized by industrials for lack of clarity concerning the definition of direct and indirect losses. Finally, this definition was revised and then arrive to a commonly agreed definition of an operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events, this definition include legal risk but exclude strategic and reputational risk" (BCPA[5], 2003).

According to Sardi (2002), "operational risk is perceived differently depending on institutions. Its perception and scope are nevertheless close and depend on institution's environment on the one hand, and the interest allowed by each actor on the other". In this context, the definition set up by Basel committee in 2004 supposes that operational risk is "the risk of loss resulting from deficiencies or defect attributable to procedures, personnel, internal system or external events".

Some banks prefer to have their own definition of operational risk. Deutsche bank (2005) defines it as "the potential for incurring losses in relation to employees, project management, contractual specifications and their documentation, technology, infrastructure failure and disasters, external influences and customer relationships". Mitsubishi Tokyo Financial Group (2005), for its part, defines operational risk as "losses sustained due to defective internal control systems and disasters and other external factors. The wide variety of risks includes those related to liquidity, operations, information security, staff management, criminal activity, transactions with customers, legal and compliance matters, disasters, reputation, and business management".

More recently, the operational risk was defined as "the risk of loss from an operational failure. It encompasses a wide range of events and actions as well as inactions, e.g., the failure to take appropriate action in a timely manner. When operational failures result in losses they are referred to as operational loss events. These losses include events ranging from unintentional execution errors, system failures and acts of nature to conscious violations of law and regulation as well as direct and indirect acts of excessive risk taking" (Op Risk Advisory & Towers Perrin, 2010).

The banks' efforts to standardize operational risk have allowed a better understanding of this issue. Indeed as noted above, the banking regulations (Basel I and Basel II) have tried not only to provide exhaustive definition of operational risk, but also to make it a prominent preoccupation of all firms given its unforeseeable consequences.

In sum, thanks to Basel agreements, operational risk was clearly defined and its scope well limited. Concerning the insurance sector, the issue of operational risk was first addressed through Solvency II regulation. However, the European Union (Directive 2009/138/EC, 2009) adopted the same definition as Basel II agreement which assumes that operational risk is "the risk of loss arising from inadequate or failed internal processes, personnel or systems, or from external events which include legal risks. This definition "excludes however risks arising from strategic decisions as well as reputation risks". Both of them are, though, treated exclusively in ORSA[6].

On the national level, operational risk is defined as "the risk of loss resulting from shortcomings and the vulnerabilities related to procedures, personnel, internal systems or external events (Moroccan Central Bank, Directive[7] No. DN29/G/2007, 2007).

2.1.2. Categorization of Operational Risk

According to Basel II agreement [WP] (2001), there are seven event types of operational risk:

- Internal Fraud: Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party (misappropriation of assets, tax evasion, intentional mismarking of positions, bribes, transactions not reported intentionally);
- External Fraud: Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law by a third party (theft of information, hacking damage, third-party theft and forgery);
- Employment Practices and Workplace Safety: Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination

[5]Basel II Compliance Professionals Association.

[6]Own Risk and Solvency Assessment: new report required by solvency directive. It includes both qualitative and quantitative aspects that show the full understanding and mastering of the risks carried.

[7]Article 56.

events;

- Clients, Products, and Business Practice: Losses arising from an unintentional or negligent failure to meet a professional obligation of specific clients (including fiduciary and suitability requirements), or from the nature or the design of a product (market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning);
- Damage to Physical Assets: Losses arising from loss or damage to physical assets due to natural disaster or other events like terrorism or vandalism;
- Business Disruption and Systems Failures: Losses arising from disruption of business or system failure (utility disruptions, software failures, hardware failures);
- Execution, Delivery, and Process Management: Losses from failed transaction processing or process management, from relations with trade counterparties and vendors (data entry errors, accounting errors, failed-mandatory reporting, negligent loss of client assets).

In summary, all these categories of risks are linked to people, processes, information system or external events.

2.2. Means Used to Address Operational Risk

The growing importance of operational risk has become largely evident in recent years, especially for companies concerned with the quality of their management but also those that want to meet the new international standards in terms of risk management. So, in order to be well equipped with tools and systems, a variety of techniques are used and continuously updated to control and manage operational risk.

Thus, the first thing to do is to define and put in place qualitative and quantitative process-based approach. On the one hand, qualitative approach aims to identify and assess operational risk, but also to increase the awareness of operational agents about risk management. On the other hand, the main objectives of a quantitative approach are to identify risk exposure and highlight the cost of operational risk.

Finally, to insure a better follow-up and good knowledge of operational risk, it is essential to link past experience through internal and external database with forward vision across risk mapping and KRI system that allow anticipating risk areas. Furthermore, permanent reporting must be ensured through risk monitoring and controlling mechanism. Each of the following sections provides details about means used for operational risk assessment and monitoring (Optimind, 2011).

2.2.1. Implementation of Internal and External Incident Database

In order to better manage future incidents, each company must be able to capitalize on previous mistakes. Accordingly, a clear and rigorous framework for collecting incidents is needed. This allows the company to create a strong risk culture but also to increase vigilance of actors. Furthermore, management and monitoring of incidents, alerts and action plans can be carried out more efficiently.

On the one hand, companies should establish internal incidents database which is progressive process. Indeed, the first step consists on collecting data related to previous incidents. It is however important to define roles and responsibilities of each one in detection of each incident. The second step concerns the definition of the perimeter of incidents that were identified in the previous step. This mainly concerns definition of the data collection thresholds, shortfalls and near-losses. Finally, methods for assessing the estimated impact of identified incidents are the subject of the last step.

On the other hand, enterprises may face extreme and scarce incidents that are not necessarily listed in their internal database. Thus, the use of external database which comprises events that have already occurred in companies operating in the same activity sector for example or in the same geographic area is highly recommended. This allows the company to better control risks by learning from others' experiences.

Commercial database in which data is public and collected from different data mediums (media, regulators, annual reports, etc.) can be used in this context. Moreover, international banks and/or insurances consortiums such ORX or ORIC in which data is collected from members anonymously can also represent a rich and reliable source of data.

2.2.2. Establishment of Control System

The control process is nothing more than the series of controls performed by the company (Bernard, Gayraud, &

Rousseau, 2006). Those controls are different according to their nature, frequencies or originators. Their main goal is to ensure the stability of the enterprise activity through:

- Insurance of enterprise integrity;
- Detection of anomalies based on abnormality of occurrence frequencies;
- Assessment of the effectiveness of the risk monitoring system and its optimization continuously.

This type of controls must be dynamic and repetitive in order to insure effective risk management which will improve company performance and sustainability.

2.2.3. Anticipation of Future Incidents

The knowledge of previous internal operational events and their related losses is not enough to have a global idea about operational risk that can occur in the future. However, the development of detailed risk mapping system leading to key risk indicator system or scenario analysis tool, provide better visibility on future risks.

1) Risk mapping

Risk mapping system allows the identification of major operational risks that can impact the company. However, their prioritization depends on multiple criteria; the most important are impact, probability, occurrence frequency and the actual level of control.

There are too many expected goals from establishing such a risk mapping system, the most significant ones are:

- Setting up an internal control system and/or risk management program;
- Enabling management to establish strategic plan and make decision when corrective actions are needed about consequent risk exposure;
- Guiding internal audit plan through highlighting major risk areas.

Risk mapping has become an indispensable tool in all companies given its power in terms of internal risk management. Therefore it is important to pay careful attention to each step of conception (Louisot & Gaultier-Gaillard, 2007). The objective is naturally to identify systematically major risks. Updates of this system are often performed annually but it can be reviewed as often as necessary when significant events occur.

2) Scenario analysis related to specific risks

Further deepening of the comprehension of the significant identified risks is made possible thanks to scenario analysis device. This allows the recognition of the probable risk paths but also the potential aggravating factors. The implementation of such a system requires high level of expertise.

This is a bottom up approach. Indeed, risks are first identified through their causes and then are mapped in each business line. They are subsequently measured-based on the frequencies of occurrence and the severity of estimated losses—either by control and monitoring indicators or by experts of each business line.

This approach completes the other tools developed in the company for risk management. Indeed, some actors use this technique only for events with low probability of occurrence and high impact; some others use this method more frequently for all types of identified incidents. This approach must be, however, well-structured and coherent in order to make effective use of subjective quantifications of risk.

3) Key risk indicators system

Monitoring of risk exposure and anticipating occurrence of risks has become possible thanks to risk indicators (Fraser & Simkins, 2011) through related warning system. Indeed, given the nature of these indicators and their evolution across time, a permanent assessment of risk and its environment can be performed. Thus, early detection of anomalies is now possible.

Defined indicators will then be summarized in dynamic dashboard that will permit for both industry players and risk managers to drive their daily decisions according to the enterprise exposure to risks.

Nevertheless, it is advisable to verify that every indicator is appropriate and understandable in order to guarantee efficiency and sustainability of the system. Furthermore, each indicator should inform about the exact exposure to each identified risk. Finally, data used in calculation of these indicators should be reliable. To end, the system should be updated as often as possible in order to have real time information.

To sum up, thanks to risk mapping which gives a precise idea about the risks incurred by the enterprise, it is possible to generate scenarios about the *future evolution of specific risks* but also to design a system of key risk indicators that *allows anticipation of risks.*

2.3. Key Risk Indicator Methodology

Key risk indicator system allows enterprise to monitor permanently its exposure to operational risk. This risk

follow up is one of the key stages in risk management process.

In this context, it should be noted that this system does not end after project design. It is intended to be an iterative process that is maintained throughout the life cycle of enterprise.

The following sections describe the five stages of risk management process (BCBS, 2003, 2011) and (Directive No. DN29/G/2007, 2007).

2.3.1. Risk Identification

All risks that could affect the achievement of enterprise objectives must be identified. This step needs a detailed analysis of transactions processing but also a deep analysis of control framework in place. Indeed, operational risk is inherent in all material products, activities, processes and systems. Risk identification involves the identification of risk sources, events, their causes and their potential consequences (ISO/Guide 73, 2009).

2.3.2. Risk Assessment

Assessment of risks consists on calculation of its financial impact and occurrence frequencies. Thanks to this step, it is possible to identify major risks that need to be managed as a priority.

2.3.3. Risk Processing

This step consists of the selection and the implementation of risk management strategy. Indeed, there are multiple means of risk management among which:

- Transferring the risk to the market or other organization;
- Reducing or eliminating the impact of risk through the implementation of an action plan that aims to improve transactions processing and strengthen control system, etc.;
- Accepting the risk without any specific action.

2.3.4. Follow up and Reporting of Risk

Risk follow-up is ensured through reportings. Indeed, they allow the whole corporate entities to monitor the evolution of their risks and to implement corrective action if required.

This risk follow up provide also information about the effectiveness of action plans put in place. If need be, other preventive or corrective actions could be proposed.

Risk monitoring should not be limited to incidents or failures but must devote close attention to proactive follow up based on control of risks by operational staff.

2.3.5. Control of Risk Management

Efficiency of risk management process should be regularly and systematically assessed by independent entity namely internal auditor or external consultants[8].

According to Scandizzo (2005) "a risk indicator is defined as an operational or financial variable that provide a reliable basis for estimating probability or severity of one or multiple operational risk events". Indeed, the main objective of these indicators is the anticipation or reduction of the effects of risks.

Monitoring, assessment and management of operational risks start by construction of key risk indicators reference framework whose major risks are drawn exclusively from risk mapping system.

2.4. Intended Objectives of the Key Risk Indicator System

The main goal of key risk indicator system is to keep staff and managers aware of risk incurred by the company. Note that several quantitative measures can be used to quantify the risk exposure (ratios, percentages and amounts, etc.).

Once these indicators reach predefined thresholds, an alarm is triggered so that preventive or corrective actions can be immediately implemented.

To sum up, the establishment of key risk indicators reporting enables companies to reach the following goals:

- Early and quick detection of risks through regular update of risk mapping;
- Reduced exposure to hazards and better risk management through a tailored plan;
- Limited operational losses.

Thus, the investment made in key risk indicator system implementation aims to contribute towards improving

[8]Steps 1 (identification), 2 (assessment) and 3 (processing) correspond to risk mapping process. The last two steps (reporting and control) are the stages needed for completing the conception of key risk indicators system.

global enterprise performance and its transactions processing through identification of appropriate measures.

2.5. Presentation and Analysis of International Standards Related to Operational Risk

In 2010, the institute[9] of operational risk has published a document (IOR, 2010) on operational risk management that focuses on best management practices recommended by IOR in order to succeed in establishing a key risk indicators system.

Furthermore, the COSO[10] (2010) has published in the same year a document on key risk indicators with recommendations for producing good indicators that enable effective enterprise risk management.

The main recommendations of these two organizations concern the selection of operational key risk indicators, setting up alert thresholds, management of operational key risk indicators and finally reporting of those indicators.

2.5.1. Control of Risk Management

Through an overview of the international standards, we will summarize the recommendations and best practices enacted by the IOR and the COSO.

1) Selection of operational key risk indicators

According to the IOR, only significant risks should be closely followed through indicators.

In this context, two approaches can be used in the operational key risk indicators selection procedure: a Bottom-up approach or a Top-down approach.

As far as the top-down approach is concerned, the top management selects the indicators that should be followed. Conversely, in the bottom-up approach, operational managers define and follow their own risk indicators.

The enterprise can choose either one or the other, or may even combine both of them (hybrid approach).

- **Characteristics of good key-indicators**

According to the IOR, the key indicators developed should fulfill the following criteria:

- Relevance: Indicators should provide relevant information about the enterprise's risk exposure;
- Measurability: Indicators should be measured accurately and regularly. The formats recommended are numbers, values, percentages or ratios. Nonquantitative indicators are subjective and could be wrongly interpreted;
- Predictability: Selected indicators should enable prediction of changes in the enterprise's risk profile in order to take preventive measures;
- Facility for monitoring: Data needed to calculate indicators should be available and affordable. Furthermore, these indicators should be relevant and easily interpretable.

A good indicator is analyzed across time in order to assess the evolution of the whole situation (profit/loss, raise/drop, etc.) and compare the company with peers (**Table 1**).

Table 1. Criteria[11] for good KRIs.

Effectiveness	Comparability	Ease of use
Indicators should	Indicators should	Indicators should
- Apply to at least one specific risk and one business function or activity	- Be quantified as an amount, a percentage, or a ratio	- Be available reliably on a timely basis;
- Be measurable at specific point in time	- Be a reasonably precise and definite quantity	- Be cost-effective to collect; and
- Reflect objective measurement rather than subjective judgment	- Have values that are comparable over time	- Be readily understood and communicated
- Track at least one aspect of the loss profile or event history, such as frequency, average severity, cumulative loss or near-miss rates; and	- Be comparable internally across businesses - Be reported with primary values and be meaningful without interpretation to some more subjective measure	
- Provide useful management information	- Be auditable; and - Be identified as comparable across organizations (if in fact they are)	

[9]This Institute was created in January 2004 in order to respond to the growing need for operational risk management, through the dissemination of standards, the exchange of information and the promotion of training.

[10]Committee of Sponsoring Organizations of the Tread way Commission.

[11](Davies, Finlay, McLenaghen, & Wilson, 2006).

Following this analysis, indicators should result in anticipative or corrective actions.

- **Management of indicators**

The management of indicators is declined in three different actions (Deleuze & Ipperti, 2013):

- Analysis of indicators which means understanding the underlying meaning of risk;
- Interpretation of indicators that consists of identifying all potential risks and determining their impact and severity;
- Identification of an action plan that will permit enhancement and correction of some issues within a predefined period of time. Furthermore, responsible for risk management should be identified in this step.

- **Determination of the number of indicators**

The number of key risk indicators depends on each company. The IOR recommend establishing neither too few nor too many indicators. The main idea is to avoid any confusion if there are too many indicators. Or in the contrary, to avoid any lack of information about real risk exposure if there are too few indicators.

These following parameters should be taken into account to decide the number of indicators to be defined:

- Number and nature of major risks identified;
- Availability of data needed to produce these indicators;
- Costs of data extraction to calculate these indicators;
- Targeted public (Operational managers, top management, executive board or others). It is generally preferred to provide operational managers with more indicators. The objective is to enable them to monitor and to control their daily activities. On the contrary, top management and executive board should receive only relevant measures because of their limited time.

With regard to identification approach, IFACI (2005)—COSO II report has recommended to map out all potential sources of each risk. The key indicators correspond to measures that enable quantification of these sources of risk.

2) Setting up of alert thresholds

If this project ended after the implementation of a set of indicators without defining a way to interpret them and action plan to prevent their impact, all these performed stages will have no value for the company. Therefore it is important to define for each monitored indicator a limit value beyond which the company should take preventive or corrective measures.

According to the IOR, risk manager need to define a normal level and a minimum threshold level for each key indicator. When this threshold is reached, a corrective or preventive action must be set up rapidly.

It is possible to define several thresholds for the same indicator. In this case, different levels of validation are needed. In fact, when an indicator reaches the first level of threshold, the operational manager can intervene alone. When the second level of the defined threshold is exceeded, the N + 1 hierarchy should undertake the necessary action.

It is important to note that the enterprise risk appetite should be taken into account when defining the alert thresholds.

3) Management of operational key risk indicators

The IOR recommends to automate manual processes for calculating indicators as far as possible, in order to avoid human errors when collecting or processing data.

However, if automatic production of indicators is not possible or if it implies high costs, company can process manually. In this case, it is appropriate to establish a procedures manual that details procedures for collecting data manually.

The institute recommends updating regularly operational key risk indicators through adding new ones or modifying the existing ones. Indeed, the ever-changing environment in which the enterprises operate obliges them to remain up to date. So, they may be faced with new risks that emerge when launching new products or new business lines. In addition, risks can also emerge from changes in the legal and/or regulatory framework.

The institute recommends also review thresholds on a regular basis. The main goal is to be sure that they are in line with the level of the enterprise' risk aversion but also that they still comply with the global strategy.

Subsequently, it is necessary to set up a procedure for the definition of events that should trigger the update of operational key risk indicators. This procedure should also explain the process used to select these indicators. Finally, this should specify particularly:

- Frequency with which key risk indicators should be reviewed;
- People or entities allowed to approve adding new indicators, changing or cancelling existing ones;

- Events that trigger update of indicators.

4) Reporting of operational key risk indicators

Operational key risk indicators system should be available to all levels of the organization. Indeed, operational managers, executive managers and board of directors should receive these indicators in the form of a personalized dashboard relevant to their needs and duties, as recommended by the institute of operational risk.

It is also appropriate to associate colors to each indicator according to its value: green for normal values, red for values above the alert threshold and orange for values between normal value and threshold.

Produced reportings should fulfill the following conditions:

- Relevance: As mentioned above, indicators should be relevant. Furthermore, great attention should be paid to reports in order to avoid producing too many and too detailed reports with a large number of indicators;
- Simplicity: Reports should not contain complicated terms, tables or mathematic formulas;
- Rapidity: Reports should be produced on a timely basis to be sure that data used in calculation is still up to date;
- Accuracy: Inaccurate metrics will misrepresent real exposure to operational risk. Thus, procedures for verifying accuracy of metrics produced should be implemented;
- Trends: Reports should indicate a clear tendency of the chosen indicators to provide an indication about their volatility and probable direction.

2.5.2. Limits of the International Standards and Practices

The existing standards and international practices which propose a general approach to manage operational risk that may seem theoretically complete are in fact not exhaustive and present some limitations:

- Absence of universal approach to identify key risk indicators. The COSO had proposed in its December 2010 publication an approach to identify risk exposure indicators. However, the committee has not referred to a methodology for identifying recognized risk. This absence of a common reference is the source of many problems when defining key risk indicators and their thresholds.
- Absence of predefined framework for identifying actors that would exploit those risk indicators. Thus, confusion may be created about the recipients of KRI dashboards: operational responsible, internal auditors or the entity in charge of risk management if it exists.
- Absence of quantitative standardization of the concept of risk aversion. Indeed, standards create a close link between key risk indicators system and risk aversion of the entity but does not provide a real framework where this subjective concept is defined clearly, in spite of its importance in the KRI system conception.
- Absence of tools and predefined guides that allow identification and quantification of thresholds.

In order to come up with real solutions to these limitations, experts and specialized institutions should focus on practical methodologies for identifying risks and actors that will deal with those risks. They should also define guides dedicated to identification and quantification of thresholds according to each business line. Indeed, the importance of risks and their associated thresholds depend not only on each company and its risk appetite, but also on their operating sector. For our part, we will propose a practical methodology for the conception of such a system in which we will try to overcome those weaknesses.

3. Process of Setting up a Key Risk Indicator System: Case of Investment Management Process

Capitalizing on the existing regulatory framework is an essential step when implementing the KRI system. However, this step is not sufficient in view of Moroccan context. We shall therefore try to identify potential difficulties prior to and during the implementation of such a system. Then, we will propose a practical approach to put it in place. Finally, this system will be applied to Investment Management Process.

3.1. Identification of Potential Difficulties during Conception and Implementation of Key Risk Indicator System

Operational key risk indicators are quantitative measures in the form of ratios, percentages, numbers or amounts that allow monitoring overall operational risk exposure. These metrics also allow proactive risk management.

However, many problems are encountered during their identification, the most common are:

- Confusion between KRI and KPI[12];
- Considerable diversity of types of risk indicators making them very difficult to identify;
- Absence of methodology to determine alert thresholds.

3.1.1. Challenges Related to Business Environment

- **Confusion between KPI and KRI**

Key performance indicators system is used as decision-making support. Indeed, this mechanism allows the evaluation of implemented measures in the light of defined targets. In practical terms, KPI system provides a number of measures that internal managers use to assess company's growth and performance depending on their predefined objectives.

In summary, KPI are means to do a diagnosis, to assess performance and to communicate about the companies realizations with respect to their set targets.

Considering the uses of the KPIs, there is a great difference with the KRIs which provide information about enterprise risk exposure and the potential changes in company's risk profile.

- **Different typologies of risk indicators**

Considering the differences in the risk profile of companies, there is no standard list of risk indicators that can be used for all companies. Therefore, each company should define its own list of indicators in order to follow up its risk exposure.

We distinguish between two types of KRIs, depending on timing of calculation, namely before or after risk occurrence:

- Key indicators of exposure: These indicators enable anticipation of risk occurrence through preventive measures. They are calculated before the occurrence of risk;
- Key indicators of proven risk: These indicators provide information about the realization of the risk and allow taking appropriate mitigation measures. They are calculated after the occurrence of the risk. We note, for instance, the number of data entry errors or the number of detected fraud.

A further distinction of indicators could be made according to their connection with one or several processes. Indeed, there are, on the one hand, specific indicators linked to a particular process. But on the other hand, there are indicators that depend on many processes at the same time such as volume of activity for example.

This diversity of indicators makes them very difficult to identify, especially with the absence of a universal methodology for indicators definition.

The COSO has admittedly proposed a methodology to define KRIs, however it presents a major limitation concerning the identification of all typologies of risk indicators.

- **Absence of methodology to determine alert thresholds**

The association of a normal value and an alert threshold with each key risk indicator is a requirement for effective use of KRIs.

When indicators display a normal value, this means that the probability of risk occurrence is weak. Therefore, no specific action is taken. On the contrary, when the value of a given indicator exceeds the set threshold, this indicates that the probability of occurrence of the underlying risk is high. In this case, corrective or preventive measures should be put in place in order to avoid or reduce potential loss. Without predefined thresholds, key risk indicators are irrelevant and difficult to interpret. It is therefore necessary to set alert thresholds for all identified risk indicators.

However, there is currently no agreed methodology to determine those thresholds. Similarly, there are no KRI dashboard templates to work with.

3.1.2. Challenges Related to the Implementation of Key Risk Indicators System

Once the operational key risk indicators are defined, their frequency of calculation are determined and their alert thresholds are set, there is still a need to establish a range of actions that are necessary to operate the KRI system:

- Automation of key indicators' calculation for those whose data is already available in the company data base;
- Definition and production of manual indicators;
- Definition of vehicles for KRI dashboards distribution;

[12]Key performance indicators

- Training of actors responsible for exploiting these dashboards.

3.2. Proposal for an Implementation Methodology of Key Risk Indicators System in Investment Management Process

3.2.1. Methodology of Identification of Key Risk Indicators

The approach we advocate for operational KRI identification consists of five steps:

Step 1: Definition of the perimeter of risks to manage

For an efficient operational risk management, the enterprise should focus on major risks. This kind of risk has a real and/or a significant potential impact on a company's financial statements.

The significance level to decide whether a risk is major or not depends on each company (revenues, results, total asset, degree of sensitivity to risks, etc.). It should be set by the top management. Thus, major risks to be followed are those whose annual impact exceeds thresholds set in fact by management.

The operational risk mapping serves as a guide to which managers can refer throughout the process of identifying company's major risks.

Step 2: Identification of KRI dashboard recipients

The second step of the KRI definition process consists of the identification of the future receivers of dashboards. Indeed, appropriate indicators should be made available to the recipients according to their functions. Relevant good practices recommend sending to each operational manager key indicators related to risks within his scope of intervention.

These indicators must be aggregated on the basis of the hierarchy level. Furthermore, they need to be available for risk manager, if there is one in the company, for internal controllers and auditors to target their checks.

Step 3: Identification of actors that would participate in indicators' definition workshop

For a successful exercise of KRI identification, it is important to involve managers who would exploit indicators in the identification workshops.

All operational managers who are responsible for managing and tracking major risks must be identified and invited to attend training sessions. The main goal of those sessions is to explain the objectives of the KRI system, the methodology for the indicators identification and thresholds setting up. The risk manager should also attend this training session in view of the important role he will play in the indicators and thresholds definition.

Step 4: Training of actors (designated in step 3) in KRIs identification methodology

Designated actors need to go through a training session dealing with identification of risk indicators process. This session should focus on:

- Definition of basic concepts: risk, major risk, key risk indicator, exposure indicator, proven risk indicator, environment indicator, specific indicator;
- Presentation of the objectives regarding the set-up of operational key risk indicators system;
- Presentation of the methodology for identification of key risk indicators and their thresholds (see step 5 below);
- Identification of people that would exploit these indicators but also those that would set up and control the KRI system;
- Presentation of the templates for KRI dashboards to produce.

Once the training session completed, a planning for holding indicators' identification workshop should be put in place.

Step 5: Holding the KRI identification and thresholds definition workshops in accordance with the predefined planning

As said above, there are two types of indicators namely, exposure indicators and proven risk indicators, calculated prior to or after risk occurrence.

In order to identify exposure indicators, it is recommended to proceed as follows:

- Identify potential sources of each selected major risk;
- Determine the indicator that would quantify each identified source of risk.

As far as proven risk indicators are concerned, the approach for indicators identification is as follows:

- Identify consequences of each selected major risk;
- Define indicator that would quantify each identified consequence of risk.

However, it is possible to combine the two types of indicators for one risk in order to ensure effective moni-

toring before and after the occurrence of risk.

In **Table 2**, we provide some examples of key indicators that managers can use for risk monitoring.

For more relevance and usefulness, indicators should meet the following requirements:

- An observed or supposed correlation between the evolution of measured phenomenon and the increase of risk;
- A stable relationship between the indicator and the measured risk, namely positive correlation between this two metrics (evolution in the same direction);
- Limits and alert thresholds correctly defined prior to the occurrence of potential events in order to implement necessary measures.

Furthermore, these indicators should be:

- Measurable on a continuous basis;
- Generated and distributed in a relatively short time in order to take rapidly all the necessary measures;
- Understandable and easily interpretable by all the recipients of dashboards.

Moreover, data needed for indicators calculation should be available and reliable. Finally, it should be taken into account that costs for indicators' implementation must be lower than the costs generated by occurrence of risks.

Within this context, it is recommended to formalize the KRI identification work in the form of data sheets that include all characteristics of each defined key risk indicator: the type of indicators (automatic or manual), the calculation frequency, the alert thresholds, the responsible for implementation, etc.

For each identified indicator, it is appropriate to establish two thresholds which may be numbers, amounts, percentages or ratios depending on the nature of the indicator:

- A threshold **L** called ***soft limit***, below which the indicator suggests that the probability of occurrence is lower than the level accepted by the company;
- A threshold **U** called ***hard limit***, above which the indicator means that the occurrence probability of the underlying risk is high.

However, each alert threshold defined should be set in consultation with the operational managers and also the risk manager of the company. In addition, the enterprise strategy and its risk aversion should be taken into account when defining those thresholds.

Once these five steps (**Figure 1**) have been completed, key risk indicators are identified and their alert thresholds

Table 2. Examples of key risk indicators.

RISKS	CAUSES/CONSEQUENCES	KEY RISK INDICATORS	KRI RECIPIENTS
- Deterioration of the work climate	- Staff turnover	- Staff turnover	Chief human resources officer
- Absence or noncompliance to safety standards	- Absenteeism	- Absenteeism rate	
- Absence of hygiene rules	- Work- related accidents	- Number of work- related accidents	
	- Rise of occupational diseases	- Number of cases of occupational diseases	
	- Deterioration of creditworthiness of a counterparty	- The average settlement period of invoices issued	- Sales manager or commercial director
- Counterparty risks	- Bad loans	- Rate of bad loans	
- Risk of depreciation of goods	- Unsold merchandise	- Merchandise inventory turnover	- Financial officer or CFO
	- Increase of inventory turnover		
- Risk of IT security	- Malicious acts of any third party	- Number of unauthorized access to enterprise IT	IT manager
	- Absence of anti-virus software installation	- Percentage of computers fitted with antivirus software	
- Risk of unavailability of systems	- Obsolescence of the computer system	- Number of IT system failure	
		- Downtime of system	

are set.

However, as specified above, there are automatic and manual indicators. The data needed to calculate the first ones is collected from the database systems of the company. On the contrary, the data needed to calculate manual indicators is drawn manually from different registers, minutes of enterprise's meetings or from external sources.

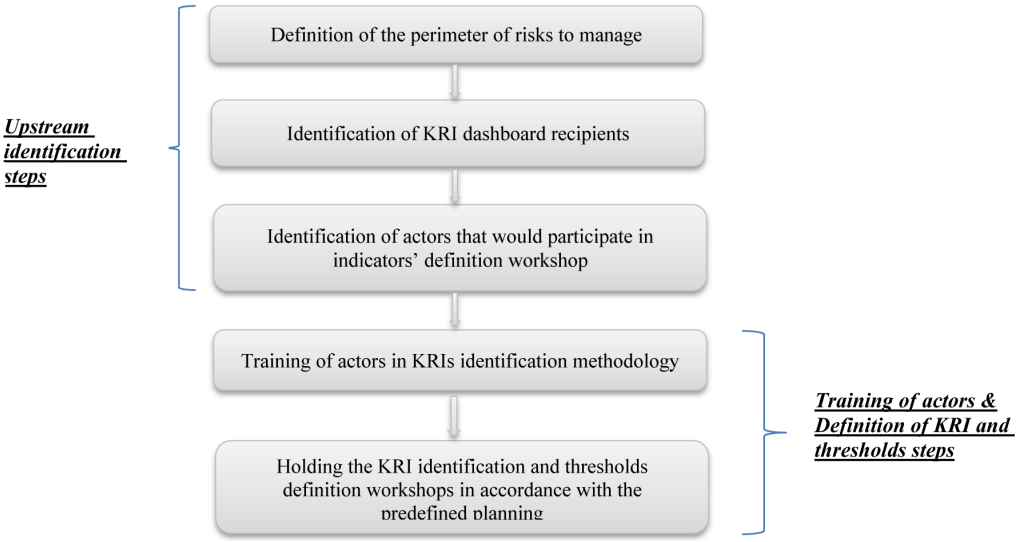

Figure 1. Summary of steps for indicators and thresholds definition.

3.2.2. Approach for Key Risk Indicators System's Implementation

After identifying operational key risk indicators and their related thresholds, we propose to proceed as follow for KRI system' implementation:

Step 1: Formalization of data processing requirements in the functional and technical specifications for the automatic production of indicators.

Those requirements depend on the needs of the company. Indeed, when it comes to the case of companies with limited resources and controlled exposure to operational risks, it is better to reduce the IT developments needed for calculating the indicators. In such a case, the following points should be indicated in the functional and technical specifications:

- The source-system data needed for indicator's calculation;
- The methodology of calculation;
- The frequency of calculation;
- The alert thresholds;
- The framework of dashboards (Immaneni, Mastro, & Haubenstock, 2004) to produce as set out in **Figure 2**.

With a view to making interpretation of the dashboards easier, it is recommended to associate a color code to each indicator (red, orange or green) as described in **Figure 3**.

On the other hand, in the case of companies with significant exposure to operational risk (insurance companies, asset management companies, banks, etc.), it may be more appropriate to develop an application dedicated to KRIs management. In addition to being used for an automatic calculation of indicators, this application can also perform the following functions:

- Provide managers with personalized dashboards;
  Allow users of indicators to propose actions with the aim of preventing or at least minimizing the exposure to risks.
- Generate synthetic and/or general reports in order to update all actors on the latest developments affecting the risk profile of the company (number of indicators that have exceeded the critical level, number of actions to implement state of the implemented measures, etc.);
- Add and/or cancel indicators to take into account the updating of risk mapping;
- Administrate the accreditations;

						Alert threshold		
Risk	Indicator	Date/ Period	Actual value	Previous value	Trend	Green	Orange	Red
Issuer risk	Issuer ratio		14%	13%	⬆	<15%	[15%-20%]	>20%

Figure 2. Template of KRI dashboard.

Red	-The value of the threshold is higher than 'U'
	-The value of the indicator is increasingly high which means a great exposure to a major risk
	- Immediate actions should be put in place to manage risk
Orange	-The value of the threshold is between 'L' and 'U'
	-The value of the indicator is higher than the normal value which means a potential exposure to a significant risk
	-Close attention is required by the management to decide whether an action should be undertaken
Green	-The value of the threshold is lower than 'L'
	-The value of the indicator is normal which means that the company is not exposed to the underlying risk
	-No action is required

Figure 3. The color code used for KRI interpretation.

- Keep a history of the changes made to the generated dashboards (modification of corrective actions for example).

Step 2: Verification of the accuracy of the automatic indicators' data and calculation

Once the necessary IT developments defined in the functional and technical specifications are completed, a test phase should be run to be sure that the calculations of indicators are correct and the obtained dashboards are consistent with the framework established. However, it is important to consider any anomaly that can be raised during the check.

Step 3: Formalization of the definition and calculation of manual KRIs

For manual indicators, the following considerations are of relevance:

- Methodology of calculation;
- Registers, reports and statements from which data needed for calculation can be extracted;
- Actors in the company in charge of calculating and producing manual indicators dashboards.

Step 4: Implementation of a procedure for operating KRIs

In order to ensure that every actor in the company is aware of his role in the operational KRI system, a procedure should be established with the aim to:

a) *Explain goals of the KRI system*, namely monitoring of major operational risk exposure but also being able to intervene rapidly in order to maintain risk exposure within the fixed limits.

b) *Identify actors and entities* that will:

- Manage and monitor the KRI system;
- Produce and distribute the KRIs dashboards;
- Exploit the key risk indicators;
- Control the relevance of proposed corrective and preventive actions and make sure that every concerned ac-

tor receives dashboards in time.

However, the correct functioning of the KRI system is ensured by the internal auditors and controllers. That is why they are allowed to access to the dashboards of the different entities. Thanks to that, they will be able to direct their control framework.

c) *Explain the actions to be conducted according to the value of each indicator*. Indeed, each manager should propose preventive and/or attenuating actions that he will validate with his hierarchy prior to implementing them if the defined thresholds are exceeded.

Furthermore, managers need to be alert to trends detected by analysis of the monitored indicators. For example, when an indicator is in the green area but its value is constantly changing to ultimately reach the red area, a preventive measure should be put in place as quickly as possible without waiting for the alert threshold to be reached.

Step 5: Training of actors responsible for operating KRIs

Once the dashboards are produced, a training session should be scheduled for all actors that will receive and use these KRIs dashboards. Indeed, they must be able to interpret the contents of such documents and take the actions needed.

Step 6: Deployment of the KRI system

Before starting a full deployment of the KRI system, it is necessary to start with pilot sites to test the system. Indeed, one or two sites should receive dashboards for managing and monitoring their major risks during a test period.

Depending on the results of the test phase, corrections should be made in case of defects.

The system will be applied throughout the company once all the technical problems will have been solved (**Figure 4**).

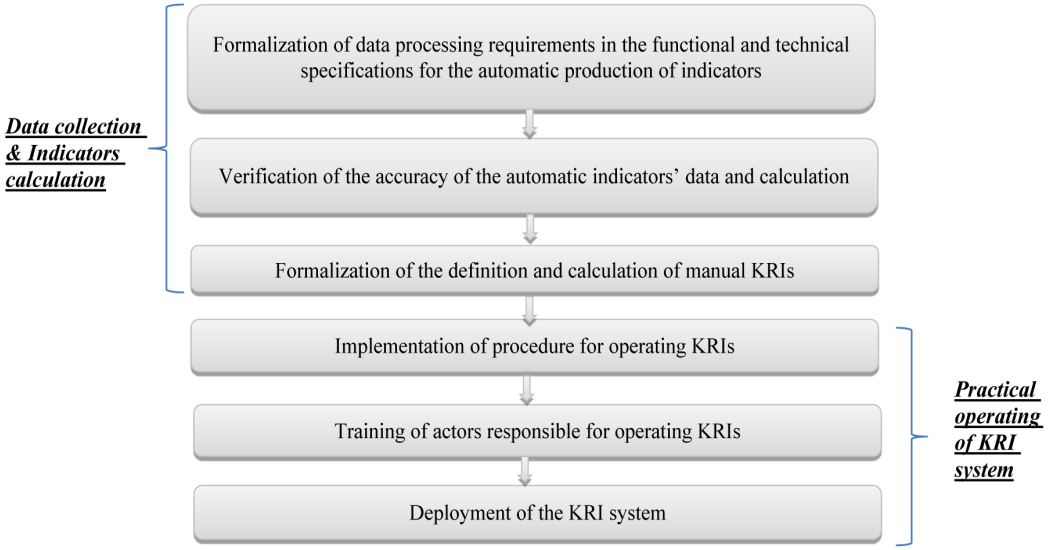

Figure 4. Steps for KRI system implementation.

3.3. Testing the Proposed Approach on Investment Management Process

Asset management is the core business in Asset Management Company. Therefore, the most important process to examine in detail is the Investment Management process. Indeed major risks can arise from this part of business. Consequently, the following sections will be dedicated to the identification of key risk indicators related to this process and the setting up of the alert thresholds.

Ultimately, an example of KRI dashboard for investment management process will be presented.

3.3.1. Identification of Key Risk Indicators Related to Investment Management Process

After performing all the stages described above including back and forth discussions with the asset managers, we have obtained the following key risk indicators as described in **Table 3**.

Table 3. Identification of key risk indicators related to investment management process.

	Risk	Possible Causes	Potential Consequences	Key risk indicators	Type of indicator
1	Insufficient unbundling of tasks between approval, execution and recording of investment accounts	- Absence of formalized procedure - Absence of strict instructions for tasks separation	- Realization of unauthorized investments - Misappropriation of funds	-The number of anomalies detected by internal controllers, internal or external auditors, etc.	Manual
2	Sub- optimized cash management: Surplus not invested, insufficient liquidity	- Bad decision-making related to cash management - Absence of investment opportunities	- Shortfall in terms of investment returns	- Theoretical return of assets not invested - Liquidity exceedance ratio.	Automatic Automatic
3	Inaccurate asset valuation	- Wrong asset prices entry - Manipulation of unlisted asset's valuation	- Money gains or losses in function of the sense of errors - Over or under valuation of unrealized gains or losses	-The number of anomalies detected by internal controllers, internal or external auditors, market authority, etc.	Manual
4	Issuer risk: Overexposure to a given issuer	Human error in: - Calculation of proportions to allocate to each issuer - Assessment of issuers	- Overtaking proportions by one issuer leading to risky exposure - Excess of the regulatory allowed level	Issuer ratio	Automatic
5	Noncompliance with the pre-established investment policy	- Human error - Absence of investment opportunities	Shortfall in terms of investment returns	Yield spread between strategic portfolio and existing one	Automatic
6	Unfunded asset's depreciation	- Human error - Inadequate analysis of the financial situation of a held asset	Incorrect financial data produced	-The number of anomalies detected by internal controllers, internal or external auditors, market authority, etc.	Manual
7	Exceedance of the borrowing limit	- Human error - Financing the overinvestment	Excess of the regulatory allowed level	Borrowing ratio	Automatic

Table 4. Setting up of alert thresholds related to investment management process.

		Alert thresholds		
Key risk indicator	**Type of indicator**	**Normal situation**	**Alarming situation**	**Critical situation**
The number of anomalies detected by internal controllers, internal or external auditors, etc.)	Manual	0	1	≥2
Theoretical return of assets not invested	Automatic	≤1% of the total investment returns	]1%; 5%[of the total investment returns	≥5% of the total investment returns
Liquidity exceedence ratio	Automatic	≤20% of the total securities portfolio[13]	]20%; 25%[of the total securities portfolio	≥25% of the total securities portfolio
The number of anomalies detected by internal controllers, internal or external auditors, market authority etc.)	Manual	0	1	≥2
Issuer ratio	Automatic	≤20% of the total securities portfolio[14]	]20%; 25%[of the total securities portfolio	≥25% of the total securities portfolio
Yield spread between strategic portfolio and existing one	Automatic	>0%	<0%	<−5%
The number of anomalies detected by internal controllers, internal or external auditors, market authority etc.)	Manual	0	1	≥2
Unrecorded depreciation value	Manual	≤1% of the securities portfolio	]1%; 3%[of the securities portfolio	≥3% of the securities portfolio
Exceedence of the borrowing limit	Automatic	≤10% of the securities portfolio[15]	]10%; 15%[of the securities portfolio	≥15% of the securities portfolio

[13]Dahir portant loi n° 1-93-213, art 78.
[14]Dahir portant loi n° 1-93-213, art 80 & 81.
[15]Dahir portant loi n° 1-93-213, art 84.

3.3.2. Setting up of Alert Thresholds Related to Investment Management Process

Once the key risk indicators were defined, several meetings were held with the portfolio managers in order to set alert thresholds, while taking account obviously of the regulatory constraints (Dahir portant loi n° 1-93-213, 1993). These have led to the thresholds described in **Table 4**.

3.3.3. Output of the Proposed Methodology

After receiving and controlling data, calculating key indicators at a frequency appropriate to their risks and finally defining alert thresholds, the remaining step consists of developing a complete dashboard that will permit continuous and more efficient monitoring of areas of risks.

In **Table 5**, there is an example of KRI dashboard for Investment Management Process that should be made available to all portfolio managers. They should complete all the fields and communicate the results to their hierarchy. A color code (green, orange or red) permits a clear identification of the state of each indicator compared to the defined threshold, but also facilitates the interpretation of dashboards.

Once the KRI system is implemented, it should be regularly updated in order to take into account all changes, whether they are internal or external.

The effectiveness of the proposed methodology can be determined once the system is fully implemented and tested over a period of at least one semester. Indeed, this period would be required for practical testing in order to have enough time for implementing preventive and/or corrective measures and finally to see the results achieved.

Table 5. Template of KRI dashboard for investment management process.

					Alert thresholds		
Underlying Risk	**Key risk indicator**	**Actual value**	**Previous value**	**Trend over the period**	**Normal situation**	**Alarming situation**	**Critical situation**
Insufficient unbundling of tasks between approval, execution and recording of investment accounts	The number of anomalies detected by internal controllers, internal or external auditors, etc.)				0	1	≥2
Sub-optimized cash management: Surplus not invested, insufficient liquidity	Theoretical return of assets not invested				≤1% of the total investment returns	]1%; 5%[of the total investment returns	≥5% of the total investment returns
	Liquidity exceedance ratio				≤20% of the total securities portfolio	]20%; 25%[of the total securities portfolio	≥25% of the total securities portfolio
Inaccurate asset valuation	The number of anomalies detected by internal controllers, internal or external auditors, market authority etc.)				0	1	≥2
Issuer risk: Overexposure to a given issuer	Issuer ratio				≤20% of the total securities portfolio	]20%; 25%[of the total securities portfolio	≥25% of the total securities portfolio
Noncompliance with the pre-established investment policy	Yield spread between strategic portfolio and existing one				>0%	<0%	<−5%
Unfunded asset's depreciation	The number of anomalies detected by internal controllers, internal or external auditors, market authority etc.)				0	1	≥2
	Unrecorded depreciation value				≤1% of the securities portfolio	]1%; 3%[of the securities portfolio	≥3% of the securities portfolio
Exceedance of the borrowing limit	Borrowing ratio				≤10% of the securities portfolio	]10%; 15%[of the securities portfolio	≥15% of the securities portfolio

4. Conclusion

The operational key risk indicators provide managers with continuously updated information in order to make the necessary adjustments for the achievement of strategic and operational targets. Thus, KRIs are powerful tools that permit anticipating the occurrence of risk (case of exposure indicators) and/or reducing its negative impact on results (case of proven risk indicators).

In addition to risk monitoring and management, KRIs enable managers to meet various other goals. Indeed, they can set concrete objectives for reducing operational risks but also increasing risk awareness of operational managers. Actually, they are accustomed to receiving KPI dashboards (the figures on sales volume, value, market share and price developments, etc.), but the same cannot be said for KRIs. Thus, receiving KRI dashboards will sensitize them on the risks that the company is exposed to, and will push them to consider this important component in their daily decisions.

Moreover, the KRI system allows the operational managers to follow the evolution of risk appetite set by the top management. Indeed, the defined alert threshold related to each key risk indicator reflects the risk appetite of the company executives, namely the amount of risk the enterprise is willing to take and is able to bear.

Finally, thanks to KRI system, it is possible to produce risk reports, either for the operational managers, the directors or the external regulators.

More recently with the increase in the operational risks, specific tools for risk management are increasingly needed especially for companies operating in financial sector. Indeed, such companies rely heavily on this kind of devices to better assess their operational risks. Thus, the main goal of this work is to propose to risk professionals, an exhaustive documentary support that will allow them to identify and anticipate the difficulties and constraints faced in general when implementing such a system. This work will also allow them to follow a practical methodology, based on the sound risk practices, to implement this system successfully.

We believe that the proposed approach will be really helpful for the operational risk management. In addition, this system can easily be adopted by companies active in different industries.

References

Basel II Compliance Professionals Association (BCPA) (2003). Basel II Accord. http://www.basel-ii-accord.com/Basel_ii_644_to_682_Operational_Risk.htm

BCBS (1998). Operational Risk Management.

BCBS (1999). *A New Capital Adequacy Framework*. Consultative Paper.

BCBS (2001). Operational Risk, Consultative Document (CD).

BCBS (2001). Working Paper on the Regulatory Treatment of Operational Risk (WP).

BCBS (2003). Sound Practices for the Management and Supervision of Operational Risk.

BCBS (2011). Principles for the Sound Management of Operational Risk.

Bernard, F., Gayraud, R., & Rousseau, L. (2006). *Contrôle interne: Concepts, Réglementation, Cartographie des risques, Guide d'audit de la fraude, Méthodologie et mise en place, Référentiels, modes opératoires*. Paris: Maxima.

British Bankers Association, ISDA, RMA, & Price Waterhouse Coopers (1999). *Chapter 4: Operational Risk the Next Frontier*. Philadelphia, PA: RMA.

COSO (2010). *Developing Key Risk Indicators to Strengthen Enterprise Risk Management: How Key Risk Indicators Can Sharpen Focus on Emerging Risks*. Research Commissioned by the Committee of Sponsoring Organizations of the Treadway Commission.

Dahir portant loi n° 1-93-213 (1993). Relatif aux organismes de placement collectif en valeurs mobilières (Modifié par la loi 53-01).

Davies, J., Finlay, M., McLenaghen, T., & Wilson, D. (2006). *Key Risk Indicators—Their Role in Operational Risk Management and Measurement*. Sydney: Risk Business International Limited.

Deleuze, G., & Ipperti, P. (2013). *L'analyse des risques: Concepts, Outils, Gestion, Maitrise*. Paris: Ed. EMS.

Deutsche Bank (2005). Annual Review.

Directive 2009/138/EC of the European Parliament and of the Council (2009). *On the Taking-Up and Pursuit of the Business of Insurance and Reinsurance (Solvency II).* Section 3, Subsection 4, Article 11, 33 and Section 4, Subsection 1, Article 101, 4 f.

Financial Security Law of France (FSL) (2003). OJ No. 177.

Fraser, J., & Simkins, B. J. (2011). *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow Executives*. Hoboken, NJ: John Wiley & Sons. http://dx.doi.org/10.1002/9781118267080

IFACI, Price Waterhouse Coopers & Landwell (2005). *Le management des risques de l'entreprise: Cadre de référence, Techniques d'application*. COSO II Report, Paris: Ed. d'Organisation.

Immaneni, A., Mastro, C., & Haubenstock, M. (2004). *A Structured Approach to Building Predictive Key Risk Indicators*. RMA Journal, Special Edition.

IOR (2010). Sound Practice Guidance on Key Risk Indicators.

ISO/Guide 73 (2009). Risk Management Vocabulary.

Louisot, J. P., & Gaultier-Gaillard, S. (2007). Diagnostic des risques: Identifier, analyser et cartographier les vulnérabilités, Afnor.

Mitsubishi Tokyo Financial Group, Inc. (2005). FORM 20-F. As Filed with the Securities and Exchange Commission.

Moroccan Central Bank (2007). Prudential Regulation, Directive No. DN29/G/2007 Relative au dispositif de gestion des risques opérationnels.

Op Risk Advisory & Towers Perrin (2010). *A New Approach for Managing Operational Risk: Addressing the Issues Underlying the 2008 Global Financial Crisis*. Sponsored by Joint Risk Management, Section Society of Actuaries, Canadian Institute of Actuaries & Casualty Actuarial Society.

Optimind (2011). Dossiers techniques d'information Optimind: Risques opérationnels.

Sardi, A. (2002). *Audit et contrôle interne bancaire* (3th ed.). Paris: Editions Afges.

Scandizzo, S. (2005). Risk Mapping and Key Risk Indicators in Operational Risk Managements. *Economic Notes, 34*, 231-256. http://dx.doi.org/10.1111/j.0391-5026.2005.00150.x

U.S. Congress (2002). Sarbanes-Oxley Act. (Pub.L. 107-204, 116 Stat. 745, enacted July 30, 2002)