International Journal for Quality Research 9(2) 243–250
ISSN 1800-6450

**Radoica Luburic** [1]
**Milan Perovic**
**Rajko Sekulovic**

**Article info:**
Received 14.03.2015
Accepted 23.05.2015

UDC – 332.05

# QUALITY MANAGEMENT IN TERMS OF STRENGTHENING THE "THREE LINES OF DEFENCE" IN RISK MANAGEMENT – PROCESS APPROACH

***Abstract:*** *The authors of the paper analyse risk management processes contained in the model considering its longstanding application in many European organisations. The paper also analyses quality management system (QMS) standards and risk management (RM) standards. It particularly addresses the process approach to QMS which, when coupled with active involvement of employees and constant improvements, makes this approach interesting as the topic of this paper. The analyses herein resulted in integrating the process approach in the "Three Lines of Defence" model with the primary objective of the model strengthening. This is to be achieved by integrating "process owner" and "risk owner" in one person or one management team in any process with its own risk.*

***Keywords:*** *Process, Risk, Process Owner, Risk Owner, Three Lines of Defence*

## 1. Introduction

Ruthless and growing competition, as well as constant changes in the market and technologies, has forced organisations to re-examine their responses to requirements and needs of users and stakeholders on continuous basis. Therefore, if they want to survive and develop, organisations have to timely recognise and adequately master more diverse and complex risks. These times of growing competition and complexity of risks, and more and more frequent and accelerated changes, have brought about an increase in the application of international quality management and risk management standards.

The authors endeavour to find the ways to strengthen risk management by applying the process approach. They start from defining (i) risk management - as coordinated activities to direct and control an organization with regard to risk (ISO Guide 73:2009, 2009) and (ii) quality management – as coordinated activities to direct and control an organization with regard to quality. This paper particularly focuses on the definition of process and process approach which says that "process is a set of interrelated or interacting activities which transforms inputs into outputs" (ISO 9000:2005, 2005).

In addition to the international standards governing the system of management, this paper finds the Three Lines of Defence model particularly important as it is the model that has been successfully applied by many European institutions for years. The premise of the Three Lines of Defence model is that each area within an

[1] Corresponding author: Radoica Luburic
email: radoica.luburic@cb-cg.org

organisation has a clearly defined and specific role in risk management and when each of these three lines of defence performs the assigned role efficiently, the likelihood that a risk will remain unrecognised and cause damage to the organization minimizes to a great extent (Risk Management: Easy as 1 2 3, 2013).

The process approach used here aims at strengthening the Three Lines of Defence model by integrating the "process owner" and the "risk owner". These two are defined as follows: the "process owner" has the responsibility and power to establish, maintain and improve the process (ISO 9004:2009, 2009), while the "risk owner" is a person or entity holding the responsibility and power to manage risk (ISO 31000:2009, 2009). The latest quality management system standard also confirms the justification of this strengthening approach by "making the risk-based contemplation on risk more explicit and integrating it into requests for establishing, application, maintaining and permanent improving of the quality management system" (ISO/DIS 9001:2014, 2014).

## 2. Core elements of the three lines of defence model for effective risk management

The Three Lines of Defence model (Figure 1) is structured so as to contain elements that are core to risk management in an organisation (Wood, 2011; Blunden and Thirlwell, 2011):

- Business line management (1st line of defence)
- Risk management (RM) function (2nd line of defence)
- Internal audit (3rd line of defence)

Business line management, as the first line of defence, manages risks in an organisation and includes mid-level and front-line management who are the risk owners responsible for the implementation and maintenance of effective internal controls.

The second line of defence is made up of professionals responsible for developing risk management methodology, providing assistance to the first line of defence in the risk identification and monitoring processes, and reporting to the management.

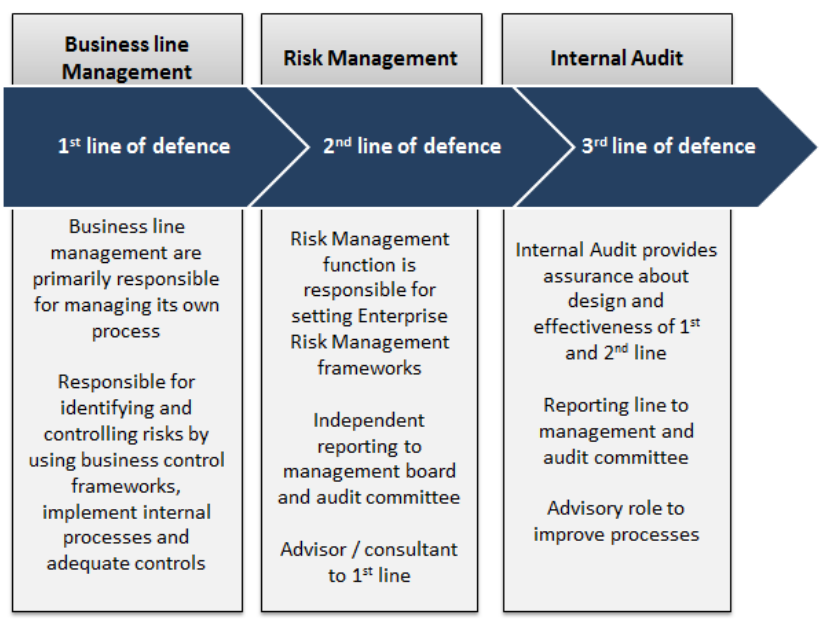


**Figure 1.** Illustration of the core Three Lines of Defence model

Internal audit, as the third line of defence, is supposed to provide reliable assurance of the risk management system efficiency in the organisation and the application of internal controls. What distinguishes internal audit from the other two lines of defence is a high level of independence and objectivity.

A particular quality of the model is that its core structure could be applied in any organisation, regardless of its size and activity. Board of directors and senior management are responsible for overseeing the strategy and risk management process and they seek assurance from different functions within the organisation in order to effectively perform their duties.

Although the basis of any good risk management is that each organisational unit in an organisation is responsible for managing risks within their competences, an integrated and comprehensive approach should be used to ensure the compliance with the organisation's objectives and strategy. To that end, the ECIIA (European Confederation of Institutes of Internal Auditing) and the FERMA (Federation of European Risk Management Organisations) supported the establishing of centralised RM function for the coordination of, and providing assistance to, risk management in an organisation (ECIIA/FERMA, 2010). Centralised RM function proposes a formal framework for risk management and implements education programmes for employees with a view to improving risk culture and understanding of risks within the organisation.

The defence mechanism in an organisation comprises three lines, thus it is very important for the internal audit to oversee the first and second lines in the manner to avoid the overlapping of activities of the other lines of defence.

In the Document titled *The Three Lines of Defence in Effective Risk Management* from 2013, the Institute of Internal Auditors (IIA) gave an overview of the Three Lines of Defence (Figure 2).

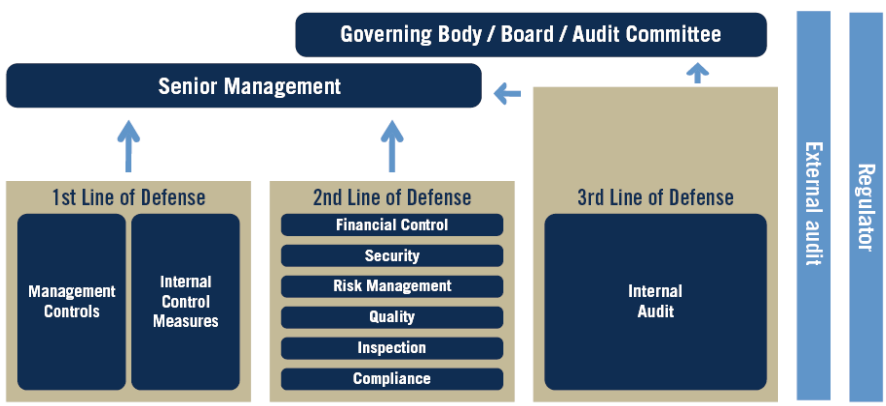


**Figure 2.** Adapted model of Three Lines of Defence (The Institute of Internal Auditors, 2013)

In order to be as effective as possible, the model requires active support of the board of directors and top management in an organisation.

The Three Lines of Defence may also be presented as follows:

- Functions that own and manage risks
- Functions that oversee risks
- Functions that provide independent assurance

Business line management, as the first line of defence, owns and manages risks. They are also responsible for performing corrective actions aimed at addressing process and control deficiencies.

Business line management is also responsible for maintaining effective internal controls and executing risk and control procedures on a day-to-day basis. It identifies, assesses, controls, and mitigates risks whilst ensuring that activities are consistent with goals and objectives. Business line management naturally serves as the first line of defence, since controls refer to systems and processes under its competence.

Since a single line of defence is often insufficient, senior management establishes various risk functions within the organisation to oversee the first line-of-defence. They vary among organizations, but typical functions in the second line of defence include risk management and compliance.

Management establishes these functions to ensure that the first line of defence is properly designed and operates as intended. Each of these functions has some degree of independence from the first line of defence, but they are by nature managerial functions. Nevertheless, internal audit is characterised by a high level of independence and objectivity, which is not available in the second line of defence. Internal audit provides assurance of the effectiveness of governance, risk management, and internal controls, and the manner in which the first and second lines of defence achieve their objectives.

External auditors, regulators, and other external bodies reside outside the organisation's structure, but they can play an important role in the risk management process. If coordinated effectively, external auditors, regulators, and other groups outside the organisation can be considered as additional lines of defence, providing assurance to the organisation's top management on the effectiveness of the first, second and third lines of defence.

The IIA recommends all three lines to be present in every organization, regardless of its size or complexity. It also notes that risk management is most effective when there are three separate and clearly identified lines of defence. Moreover, there should be proper coordination among the separate lines of defence and sharing of knowledge and information aimed at an efficient and effective risk management in an organisation.

## 3. Process approach to risk management

The process approach has been used since the first half of the 20$^{th}$ century as a way of analysing and projecting and it became the subject of international standards with the issuing of ISO 9001:2000. This approach is the basis of all approaches to total quality management (TQM) that is the qualitative upgrade to eight quality management system (QMS) principles (Perovic and Krivokapic, 2007; Krivokapic, 2011; Luburic, 2012; Luburic, 2013; Luburic, 2014; Perovic and Luburic, 2009).

International quality management standards (ISO/DIS 9001:2014) refer to the process approach as: "Consistent and predictable results are achieved more effectively and efficiently when activities are understood and managed as interrelated processes that function as a coherent system".

For the purpose of this paper, the following line of the ISO 9004 standard is also important: "For each process, the organization should appoint a process manager (often referred to as the "process owner") with defined responsibilities and authorities to establish, maintain, control and improve the process and its interaction with other processes. The process manager could be a person or a team, depending on the nature of the process and the organization's culture." (ISO 9004:2009, 2009).

International QMS standards oblige institutions to organise processes through requirements, recognise risks and integrate them into processes using planned measures, and prevent or diminish their undesired effects. What should be added here is the

obligation to involve all "process owners" into these processes, and that would necessitate their professional and job skills training, i.e. reaching necessary and desired level of competences.

These are just some of the postulates of eight QMS principles serving as the basis for TQM that may help improve the Three Lines of Defence model of effective risk management.

This begs the question of how to strengthen the Three Lines of Defence of effective risk management by applying these guideline and process approach requirements? The general answer would be – by fully infiltrating the process approach into this risk management model. This general answer may be partially presented with multiple mutually connected solutions that are complemented and strengthened with a view to more effective managing of risks.

As we have already pointed out, the premise of the Three Lines of Defence model is that each area within an organisation has clearly defined and specific roles in risk management. The primary objective is to avoid that any risk passes unnoticed, as well as to define how employees should work together and successfully manage risks.

Answers to these issues lie both in the process approach and the "process owner" who should also be the "risk owner" managing the process, who will recognise and manage risk i.e. reduce it to an acceptable level. This relation can be presented with a modified Three Lines of Defence model of effective risk management (Figure 3).

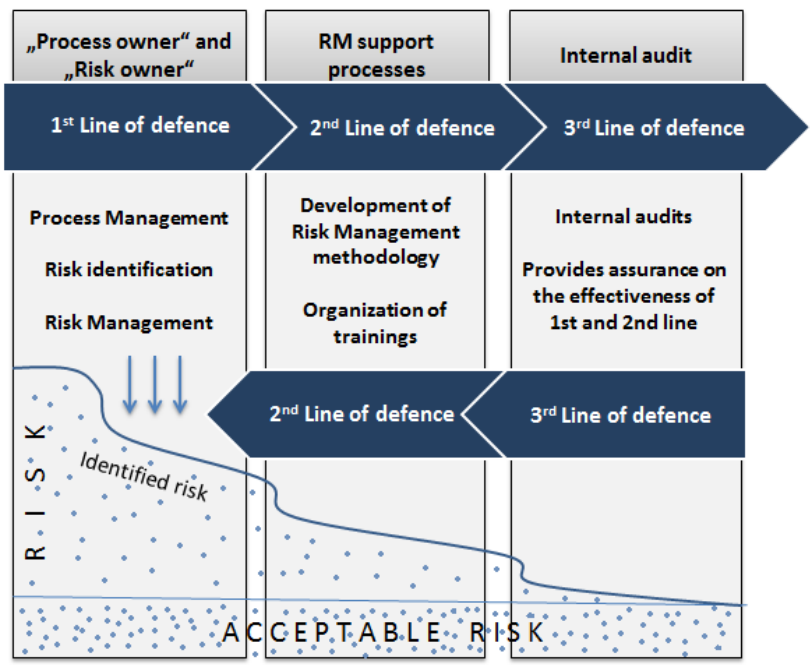


**Figure 3.** Modified Three Lines of Defence model based on the process approach

"Process owner" and "risk owner" as one person or a team is the first line of defence that fully controls risks. This immediately gives rise to questions involving senior management: What are their position, responsibility, competences and their relation to the "process owner" and "risk owner"? Are these vertical levels or

horizontal segments? The answer is that each managerial level has only those processes or network of processes that also have their "process owners" and "risk owners". The importance of classical management and hierarchy levels is lost in such internal business context of processes and process networks, and some competences of the "higher level" pass over to the "lower" level, i.e. from process networks to individual processes or from a process to its sub-processes. This enables that "higher" hierarchy structures become "flat" structures, which provides more efficient communication and management. If the "process owner" is simultaneously the "risk owner", then the relevant risk will be efficiently managed.

The paper analyses the competence segments in risk management within the Three Lines of Defence model, as well as initial requirements and obligations of the analysed segments as given in QMS standards. This particularly involves the three model segments: responsibility of the management, training, and internal audit.

The principle presented above that board of directors and senior management are responsible for overseeing the strategy and risk management process can be significantly strengthened with requirements and suggestions presented in the QMS standards: "…top management should establish and maintain a mission, a vision and values for the organization. These should be clearly understood, accepted and supported by people in the organization and, as appropriate, by other interested parties." (ISO 31000:2009, 2009) This position is further elaborated in the standards.

Then the model goes on indicating the establishing of centralised RM function for the coordination of, and providing assistance to, risk management in an organisation. Centralised RM function proposes a formal framework for risk management and implements education programmes for employees with a view to improving risk culture and understanding of risks within the organisation. These statements can be further strengthened by requirements and instructions given in the QMS standards: "The organization shall determine the knowledge necessary for the operation of its processes and to achieve conformity of products and services… The organization shall determine the necessary competence of person(s) doing work under its control that affects its quality performance (and) ensure that these persons are competent on the basis of appropriate education, training, or experience." (ISO/DIS 9001:2014, 2014).

The model view that the internal audit should oversee the first and second lines of defence should be strengthened with requirements and suggestions in the QMS standards: "Internal auditing is an effective tool for identifying problems, risks and nonconformities, as well as for monitoring progress in closing previously identified nonconformities… The outputs of internal audits provide a useful source of information for:

- addressing problems and nonconformities,
- benchmarking,
- promoting good practices within the organization, and
- increasing understanding of the interactions between processes. " (ISO 9004:2009, 2009)

The aforesaid strengthening should replace the internal audit "overseeing" function with the function "addressing problems and nonconformities".

The new issue of ISO 9001 standard requires risk-based thinking from employees where every employee is to be in charge of a process and its inherent risks. It should be highlighted here that *risk management improves process management, and process management improves risk management.*

This kind of structure offers a desirable framework for training and qualification, as well as for permanent improvements and acting based on risk-based thinking. For

processes and risk management to be successful, "process owner" and "risk owner" have to be subject to ongoing training and qualification programmes, in accordance with the adopted plan and programme. The purpose of such training is to make employees qualified to tackle and improve processes, decrease the incidents of non-conformance, and reduce risk the probability of risk appearance. All this has fostered the approach development to make constant improvements and risk-based thinking a part of organisational structure and the basis for preventive acting.

## 4. Conclusions

The obvious intertwining of principles, requirements and instructions of QMS and RM standards led the authors to develop the idea of including the QMS process approach in strengthening the model of Three Lines of Defence of effective risk management. The best way to achieve this is by merging the two institutes defined under the terms "process owner" and "risk owner" in one person or a team. In essence, the second and third lines should continually strengthen the first line of defence, particularly through the management responsibility, constant training and professional qualifications, and through internal check oriented towards addressing nonconformities, all that with a view to tackling risk detection and their diminishing through constantly improved preventive actions. Therefore, it can be concluded that risk management improves process management and vice versa through synergistic acting.

## References:


Blunden, T., & Thirlwell, J. (2011). *Mastering Operational Risk: A practical guide to understanding operational risk and how to manage it.* Great Britain: Pearson Education Limited.

ECIIA/FERMA. (2010). *Guidance on the 8th EU Company Law Directive article 41*. Brussels, Belgium.

ISO (2005). *ISO 9000:2005*. Geneva, Switzerland: International Organization for Standardization.

ISO (2009). *ISO 31000:2009*. Geneva, Switzerland: International Organization for Standardization.

ISO (2009). *ISO 9004:2009*. Geneva, Switzerland: International Organization for Standardization.

ISO (2009). *ISO Guide 73:2009*. Geneva, Switzerland: International Organization for Standardization.

ISO (2014). *ISO/DIS 9001:2014*. Geneva, Switzerland: International Organization for Standardization.

Krivokapić, Z. (2011). *Sistem menadžmenta kvalitetom.* Podgorica, Crna Gora: Pobjeda.

Luburić, R. (2012). Synergistic effects of total quality management and operational risk management in Central Banks. *International Journal for Quality Research*, *6*(4), 381–388.

Luburić, R. (2013). Challenges in Change Management in Central Banks (Based on the Systemic and Process Approach to Total Quality Management and Operational Risk Management). *Journal of Central Banking Theory and Practice*, *2*(1), 35–49.

Luburić, R. (2014). Total Quality Management as a Paradigm of Business Success. *Journal of Central Banking Theory and Practice*, *3*(1), 59–80.

Perović, M., & Krivokapić, Z. (2007). *Menadžment kvalitetom usluga.* Podgorica, Crna Gora: Pobjeda.

Perović, M., & Luburić, R. (2009). Equal distribution of knowledge: Condition for successful process approach. *International Journal for Quality Research*, *3*(1), 79–84.

Risk Management: Easy as 1 2 3 (2013, February) *IIA Newsletter - Tone at the top*. Retrieved from https://na.theiia.org/periodicals/Pages/Tone-at-the-Top.aspx

The Institute of Internal Auditors. (2013). *IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control* [Brochure]. Altamonte Springs, Florida, USA.

Woods, M. (2011). *Risk Management in Organizations: An Integrated case study approach*. New York, USA: Routledge.

**Radoica Luburic**
Central Bank of Montenegro, Montenegro
radoica.luburic@cb-cg.org

**Milan Perovic**
University of Montenegro, Montenegro

**Rajko Sekulovic**
Central Bank of Montenegro, Montenegro