Thlon, Michał

Article

Review of best international practice in operational risk management

e-Finanse: Financial Internet Quarterly

Provided in Cooperation with:
University of Information Technology and Management, Rzeszów

Suggested Citation: Thlon, Michał (2011) : Review of best international practice in operational risk management, e-Finanse: Financial Internet Quarterly, ISSN 1734-039X, University of Information Technology and Management, Rzeszów, Vol. 7, Iss. 1, pp. 13-22

MINISTERSTWO
NAUKI I SZKOLNICTWA WYŻSZEGO

eFinanse
finansowy kwartalnik internetowy

REVIEW OF BEST INTERNATIONAL PRACTICE IN OPERATIONAL RISK MANAGEMENT

Michał Thlon[1]

Abstract

The aim of this paper is to analyze standards of good practice relating to operational risk management. Huge losses incurred by renowned companies (e.g. Barings Bank, Enron) as well as local authorities (e.g. Orange County) as a result of errors in operational risk management caused growing interest in this area of science. New strategies of operational risk management implemented in companies and institutions should function within the framework created by legal and corporate regulations valid in a given country. In this paper the author presents various definitions of corporate governance standards and proposes his own definition related directly to the issues discussed here. Then he presents basic systems of risk management consistent with discussed standards. In conclusion, Polish equivalents of normative regulations discussed here were presented, on the basis of which one could construct a system of operational risk management.

JEL classification: G30, M14
Key words: operational risk, corporate governance, risk management systems

Received: 15.12.2010 Accepted: 03.03.2011

Introduction

In the past, protection against operational losses was more intuitive than formal and most frequently consisted in taking out an insurance policy and installing fire-fighting equipment (Sandgrove, 2005, p.12). Currently, due to valid regulations, a passive approach to operational risk issues is considered insufficient. Therefore, many organizations incorporated into their risk management systems some elements connected with operational risk (Waring, 2001). For the purposes of this paper we use the definition of risk compliant with the proposal of Basel Committee on Banking Supervision. It encompasses, all kinds of risk not connected directly with the volatility of the market or credit capacity of partners. It covers losses suffered due to insufficient or faulty systems, incorrect procedures and operating methods, mistakes made by people, technical break-downs, and external events (Jorion, 2007, p.553). In most cases, instead of implementing the systemic process of operational risk management, the company's efforts concentrate on improving operational efficiency. These actions mainly consist in minimizing the volatility of results achieved in particular operational processes. Although the concept of operational risk management in enterprises is still in its infancy, many scientists find it very interesting. We find the proof of this interest in numerous publications in specialist magazines and conferences, as well as in rapid development of standards relating to

[1] Michał Thlon, PhD, Cracow University of Economics, ul. Rakowicka 27, 30-910 Cracow, michal.thlon@interia.pl.

ISSUE CO-FINANCED BY THE MINISTRY OF SCIENCE AND HIGHER EDUCATION

the management of this type of risk (Raz and Hilton, 2005, pp.55-56). The system of operational risk management should function within the framework created by legal and corporate regulations valid in a given country. The point of departure for our analysis of operational risk regulations are corporate governance standards.

Corporate governance standards

The term: corporate governance should be considered in three different, but interrelated aspects formed under of historic and institutional conditionings. In the basic meaning, corporate governance is a set of rules and norms relating to a generally understood organizational management. Corporate governance may also be seen as the initiatives, developments and implementations of principles of good practice in private and public sector organizations. Yet another concept of corporate governance is to analyze it in a particular organization. It comprises individualized rules of supervision and management, also risk management (including operational risk) and relations between investors and managers.

The definition range of corporate governance standards is heterogeneous[2]. It entails mainly the OECD Principles of Corporate Governance and codifications of good corporate practice in a given country. The importance of Corporate Governance Principles lies in setting commonly accepted patterns of corporate behavior. Internal codes of good practice are the formula of transferring universal principles of OECD into specific internal reality of each member country. The term corporate governance has many meanings, because each national system of corporate governance is specific. It is a product of particular economic, legal, political, historical, social and cultural conditions. An additional determinant is the use of a particular theoretical concept, e.g. organization theory, model of stakeholders, agency theory (Sterniczuk, 2006).

The principles of corporate governance, in spite of focusing on the companies listed on the stock exchange[3], should be the tool improving the management quality in other economic entities. In some European countries the codes have been introduced even for the companies not listed on the stock exchange, for example the Belgian Buysse code. Various concepts of definitions of corporate governance standards have been presented in table 1.

Table 1: Definitions of corporate governance standards

Definition	Source
Generally corporate governance relates to the process through which organizations are directed, regulated and encouraged to report.	Australian National Audit Office, Discussion Paper, Corporate Governance in Commonwealth Authorities and Companies, 1999
Corporate governance is a system through which organizations are managed and steered	Cadbury A., The Report of the Committee on The financial aspects of Corporate Governance, 1992

[2] It means that there is no possibility to present the single, univocal and universal definition

[3] The opinion that the implementation of corporate governance principles is an effective way of improving risk management systems has been supported by the research carried out by K. Duliba in Risk Magazine, which shows that public companies are much better evaluated in this respect. See Duliba. K. (1997) *The Performance test*, Risk Magazine, November.

Corporate governance deals with minimizing transactional costs of company management	Mayer C., Oxford University, Paper written for inaugural lecture at Universite Libre de Bruxelle, February 2000
Market-focused corporate governance should be extended not only on the problems of privately-owned enterprises and on holders of huge portfolios of shares, but it should be generalized for the purpose of modeling multilateral negotiations and searching for influence among many various shareholders.	Berglof E., von Thaden E., The Changing Corporate Governance Paradigm: Implications for Transition and Developing Countries, mimeo June 1999
Corporate governance is a key element of efficiency growth and increasing investors trust	Principes de gouvernement d.entreprise de l.OCDE, OECD Publications, Paris 2004
The main idea of corporate governance is to separate the ownership rights from the control system	Morrison A.D., Sarbanes Oxley, Corporate Governance and Operational Risk, Sarbanes-Oxford Seminar, 22nd July 2004
Corporate governance determines control structure, whose main aim is to protect investors and to give them an opportunity to realize appropriate return rate from their investment as well as bringing closer the contradictory by definition interests of shareholders and managers	Monks R., Minow N., *Corporate governance*, Blackwell Business, 2004.
Corporate governance identifies the right and responsibilities, legitimates actions and determines responsibility. We can differentiate the following corporate governance activities: supervising and monitoring the effects of managers actions, responsibility, to make managers account for their actions to those who have the right to do so	Tricker R., Corporate Governance: History of Management Thought Series, 2000
Corporate governance is about the way in which managers are held responsible by shareholders and other groups and provide the company with appropriate structure to achieve this aim.	Leonard J. Brooks Business and Professional Ethics for Directors, Executives, and Accountants, 4th Edition, 2007
Corporate governance may be identified with organization of relations between the owners and corporate managers, which are complex and depend on economic conditions and national traditions.	Lannoo K., A European Perspective on Corporate Governance JCMS: Journal of Common Market Vol. 37 Issue 2, pp. 269 - 294, December 2002

Source: own work

On the basis of the definitions quoted above we may state that corporate governance standards are a set of practical means which give the management the freedom to achieve the company objectives in an efficient, effective and transparent way. In such an approach, management and governance are not the aim but the means to better results of the organization. Implementation of corporate governance principles makes the company take into account all trade and social aspects which influence its activities and aims. The effect of such actions is improvement of financial results and relations with all interest-holders (Cornall, Shapiro,

1987, pp.5-8). Examples of regulations concerning good practice of risk management are presented in table 2.

Table 2: Good Practice Standards in risk management

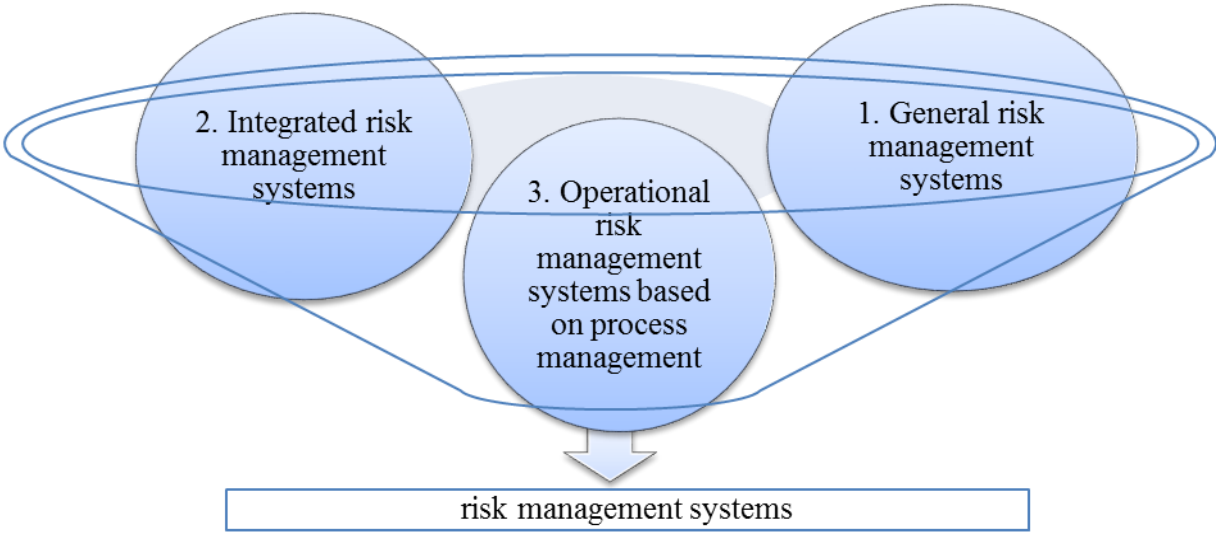
Name	Authors	Date	Scope
ISO 17799, Information Technology – Security Techniques – Code of Practice for Information Security Management	International Organization for Standardization and International Electrotechnical Commission	2005	IT risk
ISO 14001, Environmental Management Systems – Requirements with Guidance for Use	International Organization for Standardization	2004	Natural environment risk
AS 4360 Risk Management Guideline Companion	Standards Australia and Standards New Zealand	2004	All kinds of risk
Principes de gouvernement d.entreprise de l.OCDE	Organization for Economic Cooperation and Development (OECD)	2004	All kinds of risk
Enterprise Risk Management – Integrated Framework	The Committee of Sponsoring Organizations of the Treadway Commission (COSO), USA	2004	All kinds of risk
A Risk Management Standard	Federation of European Risk Management Associations (FARMA), Great Britain	2003	All kinds of risk
Sarbanes-Oxley Act (SOX)	US Congress	2002	All kinds of risk
AS 4801, Occupational Health and Safety Management System – Specification with Guidance for Use	Standards Australia and Standards New Zealand	2001	Security system risk
ISO 9001, Quality Management System - Requirements	International Organization for Standardization	2000	Risk related to quality
CAN/CSA – Q850, Risk Management Guidelines for Decision Makers	Canada Standards Association	1997	All kinds of risk

Source: own work on the basis of (King, 2001, pp.40-43), (Raz, Hillson, 2005, pp.53-66)

Risk management systems

The systems related to Good Practice Standards accepted by organizations may be arranged in three spheres presented in figure 1.

Figure 1: Risk management systems according to Good Practice Standards



Source: own work on the basis of (Samad-Khan, 2008, p.26)

General risk management systems

Models of this type contain practices supporting economic organizations in implementation of the simplest risk management systems. An example of such a regulation is the "AS 4360 Risk Management Guideline Companion" standard quoted above. This standard inspires organizations to create their language of communication related to risk issues and indicates the necessity of implementing appropriate control mechanisms. The first models of this type were used in nuclear power stations to measure the security level. According to this concept the assessment of risk level is made using the methodology based on fault tree analysis. The proposed solutions, although they do not directly indicate the type of risk, may be used in relation to operational risk[4]. The weakness of this approach is imprecise description of the risk management model (King, 1996). Its unquestionable advantage is the possibility of wide use of proposed technology in various subjects, ranging from production firms to public administration units (Keey, 2003, pp.31-32). In the risk management scheme consistent with AS4360 standard we can differentiate two basis spheres. The first one is the program of implementing risk management rules in internal structures of the organization (see figure 2). The second one is the risk management process itself (see figure 3).

[4] Conclusion on the basis of research carried out by Arthur Andersen company, which shows that implementation of AS 4360 standard allows to minimize operational loss and maximize the use of potential (Standards Australia/New Zealand, 2000).

Figure 2: Implementation program of risk management system

Source: own work on the basis of (AS/NZS 4360, 2004)

Figure 3: Risk management process with use of general standards

Source: own work on the basis of (King, 2001, p.42)

Integrated risk management systems

The concept of integrated risk management system (Enterprise Risk Management, ERM) can be defined as an approach consisting in managing risk through coordination and integration of all kinds of risks appearing inside the company (Kleffner, Lee, McGannon, 2003,pp.53-54). The definition quoted here reflects the basic aspects of integrated risk management system. In addition, this process may be characterized by identifying its most important features, namely:

1) Enterprise Risk Management is a continuous process, permeating all processes of the company's activities,
2) focus on people on every level of the organization,
3) consistency with the general strategy of the organization,
4) ability to identify potential threats,
5) dealing with risk within accepted 'risk appetite',
6) ability to provide the Board with reliable data concerning risk on all levels of activity (The Committee of Sponsoring Organizations of the Treadway Commission, 2004, p.8).

The operational risk management systems in this concept are based on the publication of The Committee of Sponsoring Organizations of the Treadway Commission (COSO) titled *"Enterprise Risk Management – Integrated Framework"*. In this concept the risk management model takes into account three dimensions. The first one is represented by the aims of the organization, considered in four perspectives:

1) strategic – the high-level aims, aligned with company mission and general strategy,
2) operations – the aims connected with efficiency and effectiveness of using resources,
3) reporting – the aims connected with information and reporting reliability,
4) compliance – the aims connected with compliance with applicable laws and regulations.

The second dimension is linking the risk management process to every aspect of the organization's activity. In this context we have the level of the unit, department, business process and supporting process. The third dimension consists of eight interrelated elements presented in detail in table 3.

Table 3: Elements of Enterprise Risk Management process

ERM components	Characteristics
Internal Environment	This stage encompasses the aspects connected with accepted philosophy and culture of risk management, ethical values and risk level acceptable by the Board
Objective Setting	Objectives must be set in compliance with the entity's strategy, its mission and risk appetite.
Event Identification	Internal and external events affecting the entity's objectives must be identified. Threats should be distinguished from potential opportunities and incorporated in the risk management process. Additional component of this stage is the analysis of relations between particular identified risk factors and general risk profile of an organization.
Risk Assessment	Consists in analyzing the impact of potential events on the goals of the process. Risks are analyzed considering likelihood and impact, and assessed both on the inherent and residual basis
Risk Response	Covers various risk responses (avoiding, accepting, reducing or sharing risks) with reference to the accepted level of risk
Control Activities	This stage checks whether accepted procedures and policies of risk management are adhered to. This refers to the whole organization, on all levels of its activities. It also covers the information and tele-communication systems control.
Information and Communication	It covers identification, collection and passing relevant information up, down and across the organization to workers of all levels of organizational structure so that they could carry out their duties concerning risk management process
monitoring	It consists in monitoring the whole process and evaluating the efficiency of its elements and the process as a whole.

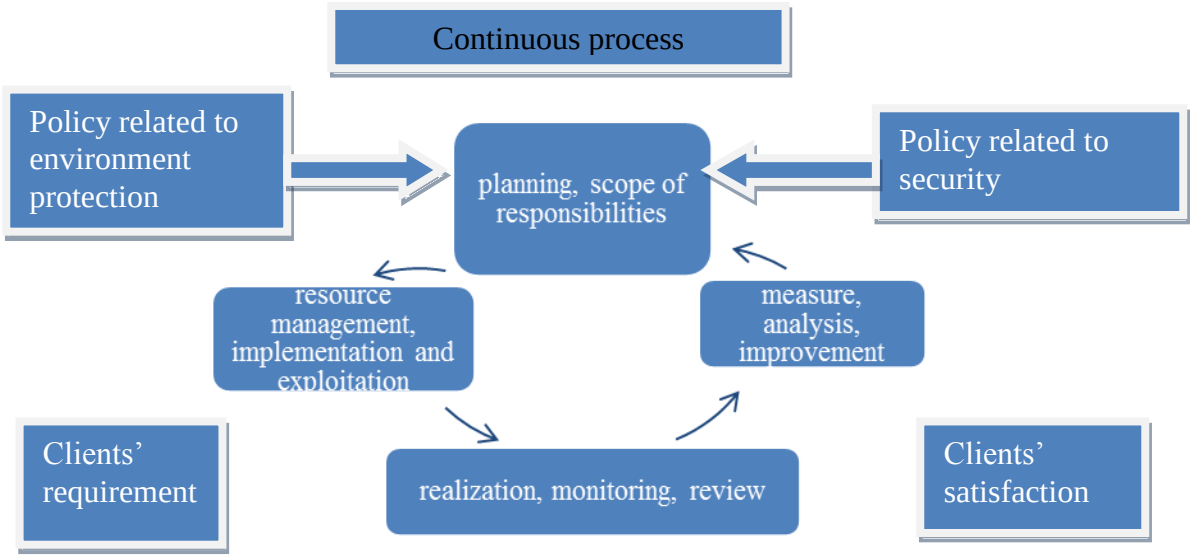
Source: own work on the basis of (COSO, 2004, p.13)

According to the research carried out in several countries, such as the USA, Canada, Australia and Europe on entities from various sectors of economy, the complete system of integrated risk management proposed by COSO was implemented by 11% of organizations (Beasley, Clune, Hermanson, 2005, pp.69-72). The biggest obstacles in implementing it were poor corporate culture and insufficient level of knowledge.

Risk management systems based on process management

Risk management systems based on minimizing losses connected with poor quality of products or services are not a new concept. Including the standards connected with safety and environment protection into quality management system is considered by specialists as a sign of pro-active policy of risk management allowing significant reduction of losses (Brumale, McDowall, 1990, pp.53-54). As an example of such a model we can quote the risk management system based on the following standards: ISO 9001 Quality Management System, ISO 14001 Environmental Management Systems and AS 4801 Occupational Health and Safety Management System. The scheme of the system based on these standards is presented in figure 4.

Figure 4: Scheme of operational risk management



Source: own work

Conclusions

The analogical model of operational risk management may also be built basing on standards valid in Poland. The equivalents of the norms quoted in the scheme above are:

1) ISO 9001 standard – Systems of quality management – referring to quality requirements demanded by organization's partners,
2) ISO 14001 standard – Systems of environment management – covering legal and non-legal requirements of environment protection,
3) PN-N 18001 standard – Systems of Health and Safety at Workplace – comprising legal requirements concerning health and safety at workplace.

ISSUE CO-FINANCED BY THE MINISTRY OF SCIENCE AND HIGHER EDUCATION

A large number of organizations using the presented standards in internal systems of risk management implemented three independent models separately for product and service quality management, safety and environment protection management (Hasan, Kerr, 2003, pp. 287-290). However, as we can deduce from the carried research[5], better effects are obtained when each of these systems in incorporated into an integrated system of risk management.

References

Australian National Audit Office, (1999). *Corporate Governance in Commonwealth Authorities and Companies*, Discussion Paper.

Baldassare, M. (1998), *When government fails the Orange County bankruptcy*, University of California Press.

Beasley M., Clune R., Hermanson D. (2005). *ERM: a report status*, Internal Auditor 62.

Berglof E., von Thaden E. (1999). *The Changing Corporate Governance Paradigm: Implications for Transition and Developing Countries*, Mimeo, June.

Brooks, L. (2007), *Business and Professional Ethics for Directors, Executives, and Accountants*, 4th Edition.

Brumale S., McDowall J. (1999). *Integrated management systems*, The Quality Magazine No.8.

Committee of Sponsoring Organizations of the Treadway Commission, (2004). *Enterprise Risk Management -Integrated Framework Executive Summary*, September.

Cornell B., Shapiro A. (1987). *Corporate Stakeholders and Corporate Finance*, Financial Management, Vol. 16, Spring.

Duliba, K. (1997). *The Performance Test*, Risk Magazine, November.

Hasan M., Kerr R. (2003). *The relationship between total quality management practices and organizational performance in service organizations*, The TQM Magazine No 15.

Jorion, P. (2007). *Financial Risk Manager Handbook*, John Wiley & Sons, New Jersey.

Keey, R. (2003). *Risk management; an Australian view*, Trans IChemE, Part B 81.

King, J. (1996). *Advanced treaty verification techniques: providing assurance on unknown activities*, Proceedings of PSAM III, referat z Probability and Safety Assessment Conference, Greece, Crete.

King, J. (2001). *Operational Risk: Measurement and Modelling*., John Wiley & Sons, Chichester.

Kleffner A., Lee R., McGannon B. (2003). *The effect of corporate governance on use of enterprise risk management: evidence from Canada*, Risk Management and Insurance Review No 16.

Kodeks nadzoru korporacyjnego dla spółek publicznych, (2002). Polskie Forum Corporate Governance, Instytut Badań nad Gospodarką Rynkową.

Lannoo, K. (2002). *A European Perspective on Corporate Governance*, JCMS: Journal of Common Market Vol. 37 Issue 2, December.

[5] See Scipioni A., Arena F., Villa M., Saccarola G., *Integration of management systems*, Environmental Management and Health, 12/2001, pp.134-145. According to these authors, the basic benefits of integrating the analyzed systems are: shortening the time period and reducing the costs of system implementation and avoiding taking into account the same risk factors twice.

Monks R., Minow N. (2004). *Corporate governance*, Blackwell Business.
Morrison, A.D., *Sarbanes Oxley, Corporate Governance and Operational Risk*, Sarbanes-Oxford Seminar, 22nd July 2004.
Principes de gouvernement d.entreprise de l.OCDE, OECD Publications, Paris 2004
Raz, T., Hillson, D. (2005). *A Comparative Review of Risk Management Standards*. Risk Management: an international journal, 7(4).
Sadgrove, K. (2005). *The Complete Guide to Business Risk management*, Gower Publishing, London.
Samad-Khan, A. (2008). *Enterprise Risk Management Modern Operational Risk Management*, Towers Perrin, Emphasis Magazine No 2.
Scipioni A., Arena F., Villa M., Saccarola G. (2001). *Integration of management systems*, Environmental Management and Health, No 12.
Standards Australia/ New Zealand (2000), *Organizational Experiences in Implementing Risk Management Practices*, Sydney.
Sterniczuk, H. (2006). *Nadzór, rozwój korporacji i satysfakcja interesariuszy*, Magazyn Top Menedżerów CEO No 4.
Szajkowski A. (2005). *Komentarz do Kodeksu Spółek Handlowych*, [w:] Sołtysiński, Szajkowski, Szumański, Szwaja t. II, wyd. 2, Warszawa.
Waring, S. (2001). *Risk ready*, Australia CPA 71(10).