Risk Management Standards in Global Markets

Luisa Bosetti
Department of Economics and Management
University of Brescia
Brescia, Italy
luisa.bosetti@unibs.it

Abstract — **Organizations face internal and external risks, which can affect their ability to achieve the established objectives and to satisfy stakeholders' expectations. However, implementing an integrated risk management system can contribute to avoid risks or reduce their consequences for corporate effectiveness. This paper describes the most important frameworks and standards of integrated risk management, emphasizing the increasing harmonization of best practices all over the world.**

Keywords – Risk; risk management frameworks and standards; integrated risk management; internal control

I. INTRODUCTION

The increasing complexity of internal and external environment exposes both private and public organizations to a multitude of risks. All organizations should properly consider such risks when they establish strategic purposes and short-term targets, because the effectiveness of governance depends on the ability to satisfy stakeholders' needs and expectations [1]. Since risks derive from natural, social, financial and organizational phenomena that could interfere with the achievement of expected results, their existence cannot be underrated [2].

In the last fifteen years, a new awareness about the relationship between risks, target setting and corporate effectiveness has contributed to spread an advanced concept of risk management. According to this view, risk management is strictly connected to both strategy setting and operations management and must be continuously carried out at all organizational levels [3], so that should create a risk management culture throughout the firm [4].

The mentioned approach is usually described as "integrated risk management" (IRM) and "enterprise risk management" (ERM) [5]. Academicians, public agencies, auditors and market regulators and supervisors have analyzed this approach [6] and recommended its adoption as a vehicle for better performances in organizations of any size and operating in any sector.

Many frameworks, guidelines and standards explain how to implement risk management in an effective way [7]. Such documents meet broad consent all over the world: this emphasizes an increasing search for harmonization of risk management practices at international level, without, however, overlooking the peculiarities of every individual organization.

Compliance with standards, guidelines and frameworks of risk management provides advantages to firms, stakeholders and supervisors [8].

a) From a *business* perspective, standards and other documents help the organization understand the complex and delicate matter of risk management, which is also subject to rapid evolution. In particular, the documents suggest how to design a risk management system and make it work properly. Moreover, they identify boards' and employees' responsibilities for well-functioning risk management processes.

b) As concern the *stakeholders*, the adoption of a universally accepted model of risk management can enhance their trust in the organization's ability to prevent damages, manage uncertainty and limit the impact of unforeseen events that could provoke losses: from a stakeholder's point of view, this is a significant assurance of corporate asset conservation and a premise for long-time value creation.

c) If an organization founds its risk management system on a broadly recognized framework, the work of *independent auditors, market supervisors, credit rating agencies, courts and any other authority with monitoring powers and duties* should be facilitated: indeed, it should consist in a comparison between the procedures and mechanisms applied by the organization and the international best practices: the higher the consistency, the more effective the implemented system.

This paper is conceptual and aims to provide an overview of the most important risk management frameworks and standards issued by different institutes and authorities. Sections II, III and IV focus on the models proposed by COSO, ISO and FERMA respectively, i.e., the most adopted international frameworks and standards of risk management. Section V describes some country-based models. Section VI concludes the paper with comparative considerations.

II. COSO'S ERM – INTEGRATED FRAMEWORK

In 2004 the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published its *Enterprise Risk Management – Integrated Framework*, which became one of the most appreciated risk management guidance for private and public organizations all over the world [9] [10]. The document is currently under review: in October 2014, COSO's board announced the project to update the *Integrated Framework*, in order to promote modifications taking in account the evolution of external environment and stakeholders' expectations. To this purpose, COSO's board appointed a group of advisors and observers composed of representatives from professional service, technological, legal, academic and public organizations, and launched an online survey. Although the survey finished in December 2014, the revision is still underway.

eISSN: 2453-7144, cdISSN: 1339-5572
ISBN: 978-80-554-1170-5

COSO's *Integrated Framework* provides a broad definition of ERM, suitable for all private and public, large and small organizations operating in any sector [11]. According to COSO, ERM is «a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives».

In other words, ERM is a continuous process, deeply rooted in the business activity and influenced by the leadership style [12]. ERM involves directors, managers and employees at every organizational level, that is to say, people with specific responsibilities of strategy setting, target planning and programming, and day-to-day operations, who differently contribute to achieve the expected results. In this sense, ERM should accompany two types of activities:

- on the one hand, the evaluation of strategic alternatives by the board of directors and top management, who need to identify the events that may impact on long-term corporate performance;
- on the other hand, the development of operational processes by the personnel, who concretely experience threats and opportunities and acquire a direct knowledge of risks.

Moreover, ERM requires that entities accept a certain degree of risk (*risk appetite*) in relation to their units (e.g., parent company and subsidiaries), functions (e.g., production, marketing, finance and human resources) and activities (e.g., manufacturing, sales, product development and accounting). A high degree of risk for a certain unit, function or activity can be accepted if it is offset by a low degree of risk for another one: the global degree of risk should always comply with the board's risk appetite, which differ among organizations. Then, the risk appetite concept must be applied to all the objectives established in plans and programs: that means identifying an acceptable range of variability (*risk tolerance*) for every result [13].

ERM should offer the board a *reasonable assurance* of achieving the established objectives, despite the uncertainty of business. More exactly, COSO's *Integrated Framework* refers to four categories of objectives: strategic; operations; reporting; compliance. According to the entity complexity, a fifth category consisting in corporate asset safeguard can be added.

COSO's approach of integrated risk management aims to improve corporate effectiveness by focusing the board's attention on the sources of uncertainty, i.e., risks and opportunities: risks are events that hamper the achievement of established targets; opportunities are phenomena the entity should exploit to reach better performances than the established ones. This relationship between risks and opportunities, on the one hand, and objectives, on the other hand, should be analyzed in a broader context, influenced by the culture of control the board of directors should promote and share with managers and employees.

To conclude, the COSO's model presents risk management as an integrated system of principles, structures and processes involving the whole entity and based on the following components [14] [15]:

- *internal environment:* the organization's rules and corporate culture, comprising risk management philosophy and risk appetite;
- *objective setting:* establishment of objectives aligned with the mission and consistent with the risk appetite;
- *event identification:* recognition of external and internal events as risks and opportunities;
- *risk assessment:* for every identified risk, analysis of likelihood of occurrence and possible impact on the organization's performance, and assessment on an inherent and a residual basis (i.e., in absence and in presence of risk response, as defined below);
- *risk response:* selection of measures to avoid, accept, reduce, or share risk, in line with the board's risk appetite and the related risk tolerance;
- *control activities:* procedures and mechanisms to ensure that the risk management system is effectively functioning;
- *information and communication:* top-down processing to divulge information about targets, risks and risk response; bottom-up processing to collect information on risks and opportunities;
- *monitoring:* comprehensive observation of the entity's ERM system, including the procedures to verify its effectiveness, in order to implement corrective actions.

III. ISO 31000:2009

ISO 31000:2009 is an international standard of risk management published by the International Organization for Standardization (ISO) in cooperation with the International Electrotechnical Commission (IEC) [16] [17]. This standard was originally issued in 2009 and is currently under review, as it is prescribed for all ISO's standards every five years.

ISO 31000 comprises two documents: *ISO 31000, Risk management – Principles and guidelines* and *ISO Guide 73, Risk management – Vocabulary*.

ISO 31000 is based on a previous guide of risk management, adopted in Australia and New Zealand in 2004 (Standard AS/NSZ 4360). Moreover, ISO 31000 is not intended for the purpose of external certification, which is typical of many other ISO standards.

ISO 31000 aims to outline an effective and efficient risk management framework for all organizations, which may properly work for any type of risks.

According to ISO 31000, risk is the «effect of uncertainty on objectives»: that means a positive or negative deviation from the expected results [18]. All entities are exposed to risks, because they cannot fully control the environment in which they operate. To increase the possibility of achieving the

eISSN: 2453-7144, cdISSN: 1339-5572
ISBN: 978-80-554-1170-5

objectives established, every organization should intervene on the likelihood of an uncertain event to happen, as well as on the consequences it would provoke in case of occurrence [19].

ISO 31000 promotes an integration of risk management and corporate governance. In this sense, risk management should be consistent with the organization's principles and values, strategies, policies, and management control, as well as with daily operations.

According to ISO 31000, risk management requires the development of several activities.

The entity should engage in a dialogue with internal and external stakeholders (*communication and consultation*) in order to:

- inform them about the risks it is exposed to and the risk management processes it has implemented, and
- collect their suggestion and feedback.

ISO 31000 stresses the importance of *establishing the context* in which risk management will be applied [20]. The term "context" must be considered in a broad sense: it refers to the internal and external environment, but also to the organization's purposes, strategies, policies, capabilities, culture, etc. When the entity establishes the context, it also selects the risk criteria against which to evaluate the significance of each risk. Risk criteria derive from the organization's risk appetite.

The next phase consists in *risk assessment*, which involves three activities:

- *risk identification:* the process of finding, recognizing and describing risks;
- *risk analysis:* the process aimed at understanding the nature and level of each risk;
- *risk evaluation:* the process of comparing the results of the risk analysis to the risk criteria, in order to determine whether a risk is acceptable.

After that, *risk treatment* is necessary for non-acceptable risks. Risk treatment measures are the following ones:

- avoiding the risk, renouncing to undertake specific activities exposed to that kind of uncertainty;
- removing the risk source;
- intervening on the event's likelihood of occurrence, on its consequences, or on both;
- sharing the risk with third parties (e.g., through an insurance coverage);
- accepting the risk by informed decision;
- taking risk to pursue an opportunity.

Furthermore, continuous monitoring and review should accompany all the steps described above: this is necessary to enable the organization to promptly react when new risks occur, internal and external conditions change, or adjustments to the original objectives are required.

IV. FERMA's Risk Management Standard

In 2003, the Federation of European Risk Management Associations (FERMA) officially endorsed *The Risk Management Standard*, a document produced the year before by three British institutes (AIRMIC, ALARM and IRM).

FERMA's *Standard* defines risk management as follows: «the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities».

According to FERMA's *Standard*, the senior management should make efforts to integrate the risk awareness into the corporate culture and to implement risk management at every organizational level: all of this is necessary to facilitate the translation of strategies into tactical and operational objectives.

Uncertain and potential events, determined by external or internal factors, can be either threats or opportunities for an entity, affecting different perspectives, such as strategic, operational and financial. Risk identification is the first step towards *risk assessment*, an activity consisting of two phases:

- *risk analysis*, comprising risk identification, description and estimation. Each risk is represented as a combination of probability of occurrence and consequence for the organization: such elements can be expressed in quantitative measures, in qualitative form, or in both;
- *risk evaluation*, during which the inherent risk is considered in the light of the organization's risk appetite.

If a risk exceeds the tolerated threshold, it must be treated. *Risk treatment* refers to different solutions for avoiding, transferring, and financing the risks by means of insurance programs, but also to several internal control procedures to prevent them or limit their consequences.

FERMA's *Standard* also recommends continuous flows of information within the organization, which are crucial for creating a complete risk map, as well as for monitoring the effectiveness of all the measures implemented to treat the risks. A risk management report should also be disseminated in the stakeholders' interest.

V. A Country-Based Analysis

In addition to the internationally accepted risk management standards, there are many country-based frameworks and guidelines, most of which have been though for listed companies: they often consist in recommendations contained in corporate governance codes and other regulations issued by the financial market regulators and supervisors.

Some countries, such as the United Kingdom, France and Canada, have published documents with specific focus on risk management. Other countries, such as China, refer to risk management in publications suggesting how to structure an effective internal control system. There are also countries, such as the US, which originally introduced risk management to reasonably assure the achievement of reporting objectives;

eISSN: 2453-7144, cdISSN: 1339-5572
ISBN: 978-80-554-1170-5

therefore, its adoption is required in compliance with the standards for auditing internal control over financial reporting.

A. The FRC's Guidance (United Kingdom)

British and foreign companies listed on the London Stock Exchange are expected to adopt the *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting*, released by the Financial Reporting Council (FRC) in September 2014. This *Guidance* revises, integrates and replaces previous documents (e.g., the *Turnbull Guidance*) in order to promote an advanced approach of risk management and internal control, taking into account the update of the *UK Corporate Governance Code* [21].

The FRC's *Guidance* describes risk management and internal control as a system of policies, culture, behaviors and processes that facilitate the achievement of operational, reporting and compliance objectives and reduce the possibility of poor decision-making.

Furthermore, the FRC's *Guidance* stresses the role of the board of directors for sharing a culture of risk management throughout the organization. Moreover, the board has the ultimate responsibility for the overall approach to risk management and internal control. In this regard, the board should:

- ensure the design and implementation of an appropriate risk management system, in which the principal risks are identified and assessed;
- determine the company's risk appetite and select the risks that should be accepted, in the light of the corporate strategies;
- agree how the principal risks should be treated in order to reduce their likelihood or impact;
- monitoring the effectiveness of the entire system and check that the corrective measures introduced for its improvement are properly functioning;
- ensure sound internal and external communication on risk management and internal control.

In particular, when the company's directors discuss about risks, they should consider several elements: for example, the nature and level of risks the organization can tolerate, the probability that such risks can happen and their impact, the possibility to implement risk response actions and their costs and benefits.

B. The AMF's Reference Framework (France)

The French *Autorité des Marchés Financiers* (AMF) published its *Reference Framework* on risk management and internal control systems in October 2010. The document is addressed to listed companies and it is still in force.

The *Reference Framework* of 2010 updated and integrated a previous edition, issued in 2007. The current edition is based on the evolution of corporate law in the EU and France; moreover, it considers the global diffusion of international standards of risk management, such as COSO's *Integrated Framework* and ISO 31000.

The AMF's *Reference Framework* defines risk as «the possibility of an event occurring that could affect the company's personnel, assets, environment, objectives or reputation». The document also describes risk management as a dynamic system of resources, behaviors, procedures and actions, «that is adapted to the characteristics of each company and that enables managers to keep risks at an acceptable level for the company».

According to the AMF, risk management contributes to:

- create and preserve the company's value and reputation;
- establish and achieve objectives;
- promote consistency between shared principles and individual conducts;
- increase the awareness of each employee about the risks involved in their activities.

According to the AMF's *Reference Framework*, an effective risk management system should respect three conditions.

a) Firstly, risk management should be found on an organizational framework designing the roles, responsibilities, procedures, policies and flows of information connected to risk management.

b) Secondly, risk management should comprise a three-stage process including the following activities: risk identification, with reference to threats and missed opportunities; risk analysis, considering likelihood of occurrence and consequences; risk response, through the selection and implementation of measures to maintain an acceptable level of risk.

c) Thirdly, the risk management system should be subject to ongoing oversight and periodic review.

Finally, the AMF's *Reference Framework* emphasizes the interaction between risk management and internal control: the risks identified by the former are submitted to procedures belonging to the latter.

C. The Canadian standard CAN/CSA Q850

Two standards of risk management, strictly connected each other, coexist in Canada. The first one is a country-based standard published by the Canadian Standards Association (CSA). The second derives from the national endorsement of ISO 31000.

The CSA originally issued its document in 1997 and reaffirmed it in 2002, with the title *CAN/CSA Q850 Risk Management: Guideline for Decision-Makers*. After the national endorsement of ISO 31000 in 2009, the CSA started the revision of its publication, which it completed in 2010. The new edition, currently in force, largely reproduces ISO 31000, as its own title stresses: *CAN/CSA Q850 Implementation of CAN/CSA ISO 31000*. However, it also underlines the need of adaptation to the social peculiarities of the Canadian context, which is marked by cultural and language differences at regional level.

eISSN: 2453-7144, cdISSN: 1339-5572
ISBN: 978-80-554-1170-5

D. Internal control models dealing with risk assessment

In some countries, the attention to risk management processes is due to their importance for implementing an adequate internal control system, as required by national laws, regulations and recommendations. For this reason, several frameworks and standards deal with both internal control and risk management, emphasizing the relationships existing between them. In this sense, China and the US offer significant examples.

On 1st January 2009, China adopted the *Basic Standard for Enterprise Internal Control*, promoted by the Ministry of Finance together with the market, banking and insurance authorities. The standard, which is mandatory for listed companies and recommended to all other large companies, requires the introduction of an internal control system including risk assessment: companies are expected to identify internal and external risk factors, evaluate their likelihood and impact, and treat them with suitable measures.

The case of the US draws attention to implementing internal control and risk management procedures in order to ensure fair and transparent financial reporting. In 2007 the Securities and Exchange Commission (SEC) approved the Auditing Standard No. 5 (*An audit of internal control over financial reporting that is integrated with an audit of financial statements*), prepared by the Public Company Accounting Oversight Board (PCAOB) in accordance with 2002 Sarbanes-Oxley Act. This auditing standard recommends a top-down approach for assessing the risk of mistakes in financial accounting and reporting. In this regard, risk assessment should enable the company to identify the accounts exposed to high risk of inaccuracy, and to check the existence of internal control procedures involving all corporate accounts (or at least the information about selected operations, such as related party transactions).

Finally, the linkage between internal control and risk management is underlined in many corporate governance codes for listed companies, where emphasis is often put on the board's responsibilities. The Italian code is a good example of this.

VI. Conclusion

The analysis presented the previous sections showed a significant harmonization all over the world in relation to the suggested practices of risk management. This is probably due to the growing global competition, which encourages the improvement of corporate governance systems as a key for supporting the company's success and the stakeholders' trust.

In particular, the three international standards and frameworks (COSO's, ISO's and FERMA's) have inspired the national ones and present substantial similarities that overtake different lexical choices (i.e., different words to express the same meaning). In this regard, Tables I-V show the similarities concerning the concept of risk, risk management phases, monitoring and review, internal reporting, and external reporting.

TABLE I. Risk Definition

COSO's ERM	Events can have negative impact, positive impact, or both. Events with a negative impact represent *risks*, events with positive impact represent *opportunities*.
ISO 31000	Risk is the *effect of uncertainty on objectives*; an effect is a deviation from the expected – *positive and/or negative*.
FERMA	Risk is the combination of the probability of an event and its consequences. There is the potential for events and consequences that constitute *opportunities for benefit* (upside) or *threats to success* (downside).

TABLE II. Risk Management Phases

COSO's ERM	• Event identification. • Risk assessment. • Risk response.
ISO 31000	• Risk assessment (including risk identification, risk analysis and risk evaluation). • Risk treatment.
FERMA	• Risk assessment (including risk analysis, risk identification, risk description and risk estimation). • Risk treatment.

TABLE III. Monitoring and Review

COSO's ERM	• *Control activities:* policies and procedures to ensure the risk responses are effectively carried out. • *Monitoring:* ongoing management activities including checks, separate evaluations, or both.
ISO 31000	• *Monitoring:* continual checking, supervising, critically observing of risk management framework, risk management process, risks and control activities. • *Review:* activity undertaken to determine the suitability, adequacy and effectiveness of risk management framework, risk management process and control activities to achieve established objectives.
FERMA	• *Reviews* to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place. • Regular *audits* to identify opportunities for improvement.

TABLE IV. Internal Reporting

COSO's ERM	*Information and communication:* • top-down processing (to share information on targets, risks and opportunities, and risk response throughout the organization) • bottom-up processing (to collect information on risks and opportunities for decision-making)
ISO 31000	*Communication and consultation* with internal stakeholders to provide, share or obtain information on risk management
FERMA	*Risk reporting and communication:* exchange of information between the board of directors, business units and individuals.

TABLE V. External Reporting

COSO's ERM	*Information and communication:* • exchange of information between entities, particularly throughout the supply chain; • dissemination of information to agencies, market supervisors, financial analysts and all other external stakeholders.
ISO 31000	*Communication and consultation* with external stakeholders to provide, share or obtain information regarding risk management
FERMA	*Risk reporting and communication* to the stakeholders to inform them about risk management policies and effectiveness in achieving objectives.

First, COSO's, ISO's and FERMA's documents share the same approach when it comes to integrating risk management with strategy setting, objective establishment and management control. Furthermore, they all consider risk management as a

pervasive process that involves and receives contribution from the whole organization. All the three documents also recommend the exchange of information about the risks between the board, top management and employees: this should create and foster a common culture of risk identification and control that is important for the adoption of a proactive behavior in relation to the uncertainty.

However, the standards of risk management seem to raise conflicting judgements. Recent surveys [22] [23] have demonstrated that many organizations, including listed companies, have no familiarity with such standards; therefore, they develop unstructured, informal and isolated risk management processes, which often consider only selected activities or corporate units.

To conclude, the factual situation suggests that standards, guidelines and frameworks of risk management can be truly effective just in culturally advanced organizations, which deeply understand the benefits provided by a global and integrated approach of risk management.

REFERENCES

[1] G. Gandini, L. Bosetti and A. Almici, "Risk management and sustainable development of telecommunications companies", Symphonya. Emerging Issues in Management, Issue 2, pp. 1-14, 2014.

[2] P. Burnaby and S. Hass, "Ten steps to enterprise-wide risk management", Corporate Governance: The International Journal of Business in Society, Vol. 9, Issue 5, pp. 539-550, 2009.

[3] J. R. S. Fraser and B. J. Simkins, "Enterprise risk management. An Introduction and overview", in Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives, J. R. S. Fraser and B. J. Simkins, Eds., Hoboken, New Jersey: John Wiley & Sons, 2010.

[4] M. Farrell and R. Gallagher, "The valuation implications of enterprise risk management maturity", The Journal of Risk and Insurance, Vol. 82, Issue 3, pp. 625-657, 2015.

[5] T. J. Andersen and P. W. Schrøder, Strategic Risk Management Practice, Cambridge, UK: Cambridge University Press, 2010.

[6] A. Nair, E. Rustambekov, M. McShane and S. Fainshmidt, Managerial & Decision Economics, Vol. 35, Issue 8, pp. 555-566, 2014.

[7] P. Bromiley, M. McShane, A. Nair and E. Rustambekov, "Enterprise risk management: Review, critique, and research directions", Long Range Planning, Vol. 48, Issue 4, pp. 265-276, 2015.

[8] L. Bosetti, "Risk management Models" (I modelli di riferimento per la gestione dei rischi, in Italian), in La gestione dei rischi e i controlli (Risk Management and Controls, in Italian), G. Gandini, Ed., Milan: FrancoAngeli, 2013.

[9] R. R. Moeller, COSO Enterprise Risk Management. Understanding the New Integrated ERM Framework, Hoboken, New Jersey: John Wiley & Sons, 2007.

[10] J. M. D'Aquila and R. Houmes, "COSO's updated internal control and enterprise risk management frameworks", CPA Journal, Vol. 84, Issue 5, pp. 54-59, 2014.

[11] B. Ballou and D. Heitger, "A building-block approach for implementing COSO's Enterprise Risk Management – Integrated Framework", Management Accounting Quarterly, Vol. 6, Issue 2, pp. 1-10, 2005.

[12] D. M. Bowling and L. Rieger, "Success factors for implementing enterprise risk management", Bank Accounting & Finance, Vol. 18, Issue 3, pp. 21-26, 2005.

[13] L. Rittenberg and F. Martens, Enterprise Risk Management. Understanding and Communicating Risk Appetite, Research commissioned by COSO, January, 2012.

[14] S. A. Lundqvist, "An exploratory study of enterprise risk management: Pillars of ERM", Journal of Accounting, Auditing & Finance, Vol. 29, Issue 3, pp. 393-429, 2014.

[15] D. M. Bowling and L. Rieger, "Making sense of COSO's new framework for enterprise risk management", Bank Accounting & Finance, Vol. 18, Issue 2, pp. 29-34, 2005.

[16] N. Baker, "Managing the complexity of risk", Internal Auditor, Vol. 68, Issue 2, pp. 35-38, 2011.

[17] D. Gjerdrum and W. L. Salen, "Standards developments", Professional Safety, Vol. 55, Issue 8, pp. 43-45, 2010.

[18] T. Aven, "On the new ISO guide on risk management terminology", Reliability Engineering & System Safety, Vol. 96, Issue 7, pp. 719-726, 2011.

[19] G. Purdy, "ISO 31000:2009 – Setting a new standard for risk management", Risk Analysis, Vol. 30, Issue 6, pp. 881-886, 2010.

[20] B. D. Gjerdrum and M. Peter, "The new international standard on the practice of risk management – A Comparison of ISO 31000:2009 and the COSO ERM Framework", Risk Management, Issue 21, March, pp. 8-12.

[21] V. Krishnaswamy, "A risky business", Accountancy, Vol. 152, Issue 1445, pp. 66-67, 2014.

[22] M. S. Beasley, B. C. Branson and B. V. Hancock, COSO's 2010 Report on ERM. Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework, Research commissioned by COSO, 2010.

[23] FERMA, FERMA Risk Management Benchmarking Survey 2012. Keys to Understanding the Diversity of Risk Management in a Riskier World, 6th ed., in partnership with Ernst & Young and AXA Corporate Solutions, 2012.