Scientific Research Publishing

Open Journal of Social Sciences, 2024, 12, 550-560
https://www.scirp.org/journal/jss
ISSN Online: 2327-5960
ISSN Print: 2327-5952

# Risk Oversight and Risk Governance of Firms

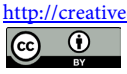
**Jiayang Cheng**

Accounting Department, Nanfang College Guangzhou, Guangzhou, China
Email: chengjiayangacca@sina.com

**How to cite this paper:** Cheng, J. Y. (2024). Risk Oversight and Risk Governance of Firms. *Open Journal of Social Sciences, 12,* 550-560.
https://doi.org/10.4236/jss.2024.1211038

**Received:** October 29, 2024
**Accepted:** November 22, 2024
**Published:** November 25, 2024







## Abstract

Risk is threats for firms' future development, so effective risk oversight is important for firms. Board of directors plays a significant role in the risk oversight process, but they are facing serious challenges and pressures in effective risk oversight. Therefore, risk governance is becoming more and more important for firms to effectively reduce their risks, develop a robust internal control system and then become profitable. In addition, risk governance is not independent itself, and its improvements also promote the further development of corporate governance and risk management, which are also important for the operation of firms. But firms' risk governance implementation also has some challenges with the development of the society; thus, this paper is aimed at providing recommendations for the better development of the risk governance.

## Keywords

Risk Oversight, Risk Governance

## 1. Introduction

Due to significant fail in some high-profile companies, many organizations are aware of the risk governance importance, and risk oversight function has become the primary objective for board (Drew et al., 2006). Recent years, the board risk oversight function has been more and more driven by external forces, such as government and risk management experts (Brown et al., 2009). And these forces place so many pressures on board directors to make them determine the most appropriate way to discharge their responsibilities in managing risks (Ittner & Keusch, 2015). Along with this situation, "risk governance theory" has been put forward as the process to manage risks and also make coordination between risk oversight outcomes and board's objectives.

Risk governance is necessary for a firm in their development. Firstly, due to more and more crisis occurrence of firms, improving risk governance and

oversight has been a priority for many organizations (Brown et al., 2009). Secondly, as a major part in corporate governance, risk governance will help to build complete corporate governance (Kumar & Sable, 2022). Thirdly, risk governance can underpin effective risk management, and sound risk management is key in all organisations (Lundqvist, 2015). However, the problem is that the practice of firms' risk governance is also facing challenges, for example, the quick development of the technology, interpersonal relationship and globalization bring opportunities and threats at the same time. Therefore, it is very important to know how to conduct effective risk governance, and this paper aims at providing insights on the better development of risk governance in practice.

## 2. Risk Oversight

Risk oversight is the term used by SEC (United States Securities and Exchange Commission) rule on proxy disclosure enhancements. According to Fraser (2016), risk oversight describes the role of the board directors in the risk management process. Risk oversight is almost involved in all aspects of organizations (Goldberg & Harsch, 2010).

### 2.1. Role of Borad of Directors in Risk Oversight

A firm's board of directors plays a critical role in overseeing an enterprise-wide approach to risk management (Wu & Wu, 2014). Following are six main roles of them: oversight, monitoring, interaction with management, approve and review, third-party review, independence and board composition.

First of all, the most obvious role of directors is oversight, through which the board's understanding and involvement in all matters concerning the strategy, risk appetite, and conduct of the firm, and an understanding of the risks it faces and its resiliency can reach (Goldberg & Harsch, 2010). Secondly, board directors take charge of monitoring. This monitoring process need to comply with the agreed strategy and risk appetite and with all applicable laws and regulations. Meanwhile, Board directors' monitoring process can also help organization proactively follow up on potential weaknesses or issues (Goldberg & Harsch, 2010). Thirdly, as indicated by Committee of Sponsoring Organizations (COSO), directors should be responsible of interacting with management. This helps to create a robust challenge to the management through a discussion of all strategic proposals, key risk policies, and major operational issues. Fourthly, also as said by COSO, directors are responsible for approve and review key policies, business objectives, strategy and plans, risk appetite framework, appointment and performance review/compensation of the CEO, senior management. Moreover, the Board is also expected to approve the mandate, resources (amount and type) and budgets for the oversight functions. Fifthly, Protiviti Global Business Consulting indicates that directors need third-party review. Specifically, the board should occasionally conduct a self-assessment with the assistance of independent external advisors to assess the effectiveness of board and committee governance practices, including

incorporating tools such as a competency matrix. Then, boards should also occasionally conduct a benchmarking analysis of oversight functions with the assistance of independent external advisors. In addition, according to Ernst & Young (EY), directors should remain independent, which means roles of chair and CEO should be separated. Furthermore, approval of director independence policy should take into consideration the specific ownership structure of the institution. Where appropriate, director tenure should also be factored into the independence policy. Last but not least, Protiviti Global Business Consulting also shows that directors are responsible for board composition like recruiting members who collectively bring a balance of expertise, skills, experience, and perspectives and who exhibit irreproachable independence of thought and action.

### 2.2. Challenges of Risk Oversight

Nowadays, with the quick development of the risk oversight, it has already become a high priority and primary board objective for companies' board of directors (Caldwell, 2012). However, at the same time, as indicated in International Risk Governance Council (IRGC), the role of the board of directors in enterprise-wide risk oversight has become increasingly challenging as expectations for board engagement are always high.

Following are the challenges that are encountered by board in the risk oversight. Firstly, most of the members in the board do not have professional training, skills and experience on enterprise risk management (ERM). Although they are excellent managers of firms, they are just based on their instinct. For example, they do not know how to apply principles in managing firms' risks with customers, employees and suppliers. Hence, it is eager for board members to possess the professional knowledge about the risk management (Fraser, 2016). Secondly, board members are confused about what the risk is. Many risk management departments in firms are only responsible for buying insurance for some identified risks and only about 25% of the firms are really conducting risk management (Fraser, 2016). Thirdly, board members do not have in-depth understandings about the risk, for example, some high regulated industries are required to fill forms to demonstrate compliance with regulations, thus, they do not really focus on the risks and consolidate the risks in the reality (Fraser, 2016). Finally, another challenge faced by board is how to effectively oversee the organization's enterprise-wide risk management in a way that balances managing risks while adding value to the organization (Goldberg & Harsch, 2010). Relevant survey indicated that there is still room to improve risk oversight. To begin with, there are still financial service organizations that consider risk oversight as a full-board function and don't have a dedicated risk management committee. In addition, for efficiency, boards often allocate oversight of specific risks to their board committees (Caldwell, 2012). However, the survey shows a significant number of directors (37%) believe there is no clear allocation of specific responsibilities for overseeing major risks among the board and its committees (or are not sure whether there is any such

allocation). Besides, many directors may understand the risks the company faces, but they are not sure who on the board is supposed to oversee them (Caldwell, 2012). Lastly, as indicated by IRGC, this structural disconnect could prove troublesome for companies in the long run.

## 3. Risk Governance

### 3.1. What is Risk Governance

In order to control the risk of firms, risk governance is necessary (Stein et al., 2019). Wikipedia indicates that risk governance is defined as a translation of the substance and core principles of governance to the context of risk and risk-related decision making. According to Renn (2008), risk governance refers to activities requiring consideration of legal, institutional, social and economic contexts in which a risk is evaluated, and involvement of the actors and stakeholders who represent them. According to IRGC, risk governance deals with the identification, assessment, management and communication of risks in a broad context. It includes the totality of actors, rules, conventions, processes and mechanisms and is concerned with how relevant risk information is collected, analysed and communicated, and how management decisions are taken. According to Wikipedia, risk governance goes beyond traditional risk analysis to include the involvement and participation of various stakeholders as well as considerations of the broader legal, political, economic and social contexts in which a risk is evaluated and managed. Moreover, scope of risk governance also encompasses public health and safety, environment, old and new technologies, security, finance, and many other factors as indicated in IRGC.

According to IRGC, good risk governance includes transparency, effectiveness and efficiency, accountability, strategic focus, sustainability, equity and fairness, respect for the rule of law and the need for the chosen solution to be politically and legally feasible as well as ethically and publicly acceptable. In addition, good risk governance also enables societies to benefit from change while minimising the negative consequences of the associated risks because risk always accompanies change. Furthermore, sound risk governance minimises the following issues: inequitable distribution of risks and benefits between countries, organisations and social groups; differing approaches to assess and manage the same risk; excessive focus on high profile risks, to the neglect of higher probability but lower profile risks; inadequate consideration of risk trade-offs; failure to understand secondary effects and linkages between issues; cost of inefficient regulations; decisions that take inappropriate account of public perception; loss of public trust.

There are two important elements in risk governance: risk appetite and reporting. According to Wikipedia, risk appetite is the level of risk that an organization is prepared to accept, before action is deemed necessary to reduce it. According to Oterholm (2024), the definition of risk appetite is different across various systems and organizations, and ISO (2022) guide defines risk appetite as the amount and type of risk that an organization is willing to pursue or retain. It represents a

balance between the potential benefits of innovation and the threats that change inevitably brings. As for reporting, Wikipedia indicates that it assesses the level, quality and adequacy of risk information provided to the directors to ensure understanding of existing and emerging risks. Besides, it also assesses the robustness of risk information technology systems and their ability to generate timely, comprehensive, cross-geography, cross-product information on exposures. risk reporting is the tool to communicate the value which risk function brings to a firm, it enables proactive risk management when organisations take a proactive approach to managing risk by identifying and escalating issues as they arise or before they are realised (PWC, 2011).

### 3.2. Risk Governance Frameworks

IRGC has developed a comprehensive framework for risk governance, and according to IRGC, risk governance framework is a comprehensive approach to help understand, analyse and manage important risk issues for which there are deficits in risk governance structures and processes. The framework offers two major innovations to the risk field: the inclusion of the societal context and a new categorisation of risk-related knowledge. Besides, it also discusses wider governance issues such as organisational capacity and regulatory styles.

Following are core of the IRGC Framework: five linked risk governance phases. Phase 1 is pre-assessment. Risk governance framework can provide risk pre-assessment. Specifically, it gives an early warning and framing of the risk, which can help to provide a structured definition of the problem, of how it is framed by different stakeholders, and of how it may best be handled. Phase 2 is appraisal. Risk governance framework offers risk appraisal. More specific, it combines a scientific risk assessment (of the hazard and its probability) with a systematic concern assessment (of public concerns and perceptions) and then provides the knowledge base for subsequent decisions. Phase 3 is characterisation and evaluation. It helps with characterisation and evaluation in which the scientific data and a thorough understanding of societal values affected by the risk are used to evaluate the risk as acceptable, tolerable (requiring mitigation), or intolerable (unacceptable). Phase 4 is management. Risk governance framework is helpful for risk management. It tells companies the actions and remedies needed to avoid, reduce, transfer or just retain the risk. Phase 5 is communication. It provides frameworks about risk communication. For example, it tells organization how stakeholders and civil society understand the risk and participate in the risk governance process.

Following are some benefits of adopting risk governance framework. Firstly, the IRGC framework is innovative, comprehensive and flexible. Specifically, it offers guidelines for identifying, understanding and addressing the essential elements of sound risk governance. Besides, it can help risk governance institutions to structure their tasks. Moreover, it can assist in diagnosing deficits in the risk governance process and provide suggestions for how to correct them. Internationally, the framework can add to efforts to harmonise risk governance approaches

and find common denominators for risk handling in a globalised and plural world. Secondly, the framework can encourage people to raise the relevant questions, whose answers will help reduce uncertainty and increase the capacity to deal with the unanticipated and the unknown. Thirdly, besides risk assessment, management and communication (standard elements of risk handling), the IRGC framework also incorporates additional activities which reflect the need to deal with risk in a way that fully accounts for the societal context of both the risk and the decision that is reached. Fourthly, IRGC has emphasises on crucial role of communication. This includes informing people of a risk and also establishing the two-way dialogue needed at all stages of the risk handling process. Excellent communication is particularly important for the involvement of stakeholders in participative risk-related decision making and conflict resolution and for ensuring that they can make informed choices about the risk, balancing factual knowledge about it with their own interests, concerns, beliefs and resources. Fifthly, the framework offers an interdisciplinary and multi-level governance approach. Most notably, it urges risk governance institutions to gather not only knowledge about the physical impacts of technologies, natural events or human activities but also knowledge about the concerns that people associate with these and other causes of risks. Finally, the framework is not intended as a recipe or a checklist which can guarantee that all relevant aspects are considered when analysing a risk and its governance process and structures. It cannot replace thinking or, for that matter, creativity. However, by building into conventional risk analysis and management such "soft" issues as societal values, concerns and perceptions of risk and by looking into the interactions between the various actors involved in the process, the IRGC risk governance framework can contribute to the development of more inclusive and effective risk governance strategies.

### 3.3. Necessity of Risk Governance

Risk governance is necessary because it does not only help to reduce firms' risks and it also facilitate the development of corporate governance and risk management, which are also fundamental for firms' development and survive (Khan, 2011).

#### 3.3.1. Promotion of Risk Governance on Corporate Governance

According to Investopedia, corporate governance is defined as a system of rules, practices and processes by which a company is directed and controlled, it is aimed at balancing the interests of many stakeholders (shareholders, management, customers, suppliers, financiers, government and the community) within the company. In a narrow term, corporate governance refers to the relationship between a firm and its shareholders, whereas in a broader term, it means the relationship between a firm and the whole society (Li et al., 2019). Furthermore, since corporate governance also offers the framework for attaining a companies' objectives, it encompasses almost every aspect of management: action plans, internal controls,

performance measurement and corporate disclosure. Good corporate governance is fundamental to the whole economies, and it also facilitates firms' success (Khan, 2011).

Due to some significant accounting fraud bankrupted in high-profile companies such as Enron and WorldCom, corporate governance becomes a pressing issue because most companies strive to have a high level of corporate governance to avoid accounting fraud (Dorfman, 2004). These days, it is not enough for a company to merely be profitable, company also needs to demonstrate good corporate citizenship through environmental awareness, ethical behaviour and sound corporate governance practices (Birch, 2017).

According to COSO, risk governance is one of the major parts and process in corporate governance, risk governance will help to build complete corporate governance. Thus, it is necessary and important to facilitate the development of risk governance.

#### 3.3.2. Promotion of Risk Governance on Risk Management

According to International Organization for Standardization, risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. According to Wikipedia, objective of risk management is to assure uncertainty does not deflect the endeavour from the business goals. As said in Echelon, there are many strategies to manage risk such as transferring the risk to another party, avoiding the risk, reducing the negative effect or probability of the risk, or even accepting some or all of the potential or actual consequences of a particular risk.

ISO 31000 is a family of standards relating to risk management codified by the International Organization for Standardization. The purpose of ISO 31000 is to provide principles, frameworks, process and generic guidelines on risk management. ISO 31000 seeks to provide a universally recognised paradigm for practitioners and companies employing risk management processes to replace the myriads of existing standards, methodologies and paradigms that differed between industries, subject matters and regions. ISO 31000 can be used by any organization no matter what size, activity or sector, which help organizations to increase the likelihood of achieving objectives, improve the identification of opportunities and threats, effectively allocate and use resources for risk treatment, and provide guidance for internal or external audit programmes. By using ISO 31000, firms can compare their risk management practices with an internationally recognised benchmark, providing sound principles for effective management.

According to Wikipedia, risk management is what management does, which includes appropriate oversight and monitoring to ensure policies are carried out and processes are executed in accordance with management's selected performance goals and risk tolerances. Thus, based on the above definition of risk management put forward by International Organization for Standardization, it can be

seen that there are overlapping in the concepts between risk management and risk governance, risk governance promotes the development of risk management. Therefore, it is evident that the necessity of facilitating the development of risk governance.

Based on the above analysis, it can be seen that it is necessary to conduct risk governance since it can help to improve the development and establishment of the corporate governance and risk management, which are both crucial for firms. However, the risk governance is still impeded by some challenges as indicated following.

### 3.4. Challenges of Risk Governance

Move into 21st century, risk governance faces so many challenges. In the context of globalisation, today's world has some characteristics such as increasing interconnectedness, social networking and fast-paced technological change (Passaris, 2006). As indicated by IRGC, along these characteristics, there are also opportunities which may potentially increase vulnerabilities and create new risks with much larger scale impacts and over longer period. More specifically, because the evolution of governance mechanisms occurs much more slowly than driving technological and social change process, several serious concerns and suspicions from governments, the private sector, as well as the general public appear. They think there are lack of governance mechanisms in terms of dealing with risks efficiently, resolving trade-offs between diverse needs and interests, dealing with potential risks from new technologies in the context of global trade. Therefore, policy makers have subsequently become increasingly conscious of the importance of risk communication and try their best to meet public expectations regarding risk governance.

## 4. Recommendations for Risk Governance

From above analysis, it can be seen that firms are still facing risk in their daily operating, so the risk oversight is of great importance and the risk governance is necessary. However, there are some challenges for risk governance, thus, this paper put forwards some recommendations for firms' better development of risk governance.

According to ISO 31000, following are five attributes representing a high level of performance in managing risk, which can assist organizations to improve risk governance implementation. These attributes are recommended to help organization have a current, correct and comprehensive understanding of its risks and make sure organization's risks are within its risk criteria. Firstly, companies should make continual improvement in risk governance by setting organizational performance goals, measurement, and review. Besides, subsequent modification of processes, systems, resources, capability and skills are also needed. For example, organization needs to measure organizations' and individual manager's performance against explicit performance goals. Then, annual review of performance,

revision of processes and the setting of revised performance objectives need to be established. This performance assessment is very important because it is an integral part of the overall organization's performance assessment and measurement system for departments and individuals.

Secondly, companies should enhance risk governance through setting comprehensive, fully defined and fully accepted accountability for risks, controls and risk treatment tasks. Specifically, designated individuals who fully accept accountability are appropriately skilled and have adequate resources to check controls, monitor risks, improve controls and communicate effectively about risks and their management to external and internal stakeholders. For instance, all staffs within an organization should be fully aware of the risks, controls and tasks that they are accountable. Meanwhile, this information is recorded in job descriptions, databases or information systems. Full accountability for risks is very important because accountabilities and responsibilities should be part of all the organizations' induction programmes.

Thirdly, when companies make decisions, they should be aware of that all decision making within the organization involve the explicit consideration of risks and the application of risk governance to some appropriate degree no matter what level of importance and significance. For example, records of meetings and decisions can show that explicit discussions on risks take place. In addition, these records also indicate that all components of risk governance are represented within key processes for decision making in the organization. This attribute is of great importance because soundly risk governance can be seen within the organization as providing the basis for effective governance.

Fourthly, companies should enhance risk governance by continual communications with external and internal stakeholders. These continual communications include comprehensive and frequent reporting of risk management performance. Take communication with stakeholders an example, it is an integral and essential component of risk governance. It also should be noted that this communication is seen as a two-way process because through communications, not only properly informed decisions can be made but also comprehensive risk criteria can be established. Comprehensive and frequent external and internal reporting is very important because they all contribute to effective governance within an organization.

Finally, it is important for companies to know that risk governance is regarded as central of the organization's management processes, which means governance structure and process are based on the governance of risk. Therefore, effective risk governance is viewed as essential for the achievement of the organization's objectives. For example, managers' language and important written materials in the organization using the term "uncertainty" are always related to risks. Furthermore, this attribute is often reflected in the organization's statements of policy, especially those relating to risk governance. Normally, this attribute would be verified through interviews with managers and through the evidence of their actions and statements.

## 5. Conclusion

In conclusion, firms are gradually realizing the importance of risk oversight in the daily operation because of the frequent exposure of the high-profile fraud like Enron and WorldCom. Board of directors in firms play significant role in risk oversight including oversight, monitoring, interaction with management, approve and review, third-party review, independence and board composition, and they are facing increasing challenges in this process. Thus, in order to maintain an effective risk oversight within the firms, risk governance is necessary, and the implementation of risk governance also promotes the improvement of corporate governance and risk management. However, nowadays firms' risk governance is also facing some challenges in the implementations. Therefore, five recommendations (making continual improvement in risk governance by setting organizational performance goals, measurement, and review; setting comprehensive, fully defined and fully accepted accountability for risks, controls and risk treatment tasks; being aware of that all decision making within the organization involves the explicit consideration of risks; continual communications with external and internal stakeholders; governance structure and process should be based on the governance of risk) are put forward to make better development for firms' risk governance.

## Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

## References

Birch, D. (2017). Corporate Citizenship: Rethinking Business beyond Corporate Social Responsibility. In J. Andriof, & M. McIntosh (Eds.), *Perspectives on Corporate Citizenship* (pp. 53-65). Routledge. https://doi.org/10.4324/9781351282369-4

Brown, I., Steen, A., & Foreman, J. (2009). Risk Management in Corporate Governance: A Review and Proposal. *Corporate Governance: An International Review, 17,* 546-558. https://doi.org/10.1111/j.1467-8683.2009.00763.x

Caldwell, J. E. (2012). *A Framework for Board Oversight of Enterprise Risk*. Canadian Institute of Chartered Accountants.

Dorfman, J. (2004). *What Enron, WorldCom, Tyco Fiascos Can Teach Us*.

Drew, S. A., Kelley, P. C., & Kendrick, T. (2006). CLASS: Five Elements of Corporate Governance to Manage Strategic Risk. *Business Horizons, 49,* 127-138. https://doi.org/10.1016/j.bushor.2005.07.001

Fraser, J. R. (2016). The Role of the Board in Risk Management Oversight. In R. Leblanc (Ed.), *The Handbook of Board Governance: A Comprehensive Guide for Public, Private and Not-for-Profit Board Members* (pp. 283-313). John Wiley and Sons, Inc.

Goldberg, L., & Harsch, M. (2010). *Director Notes: The Role of the Board in Risk Over-Sight*. The Conference Board.

ISO 31073:2022(en) (2022). *Risk Management—Vocabulary*. https://www.iso.org/standard/79637.html

Ittner, C. D., & Keusch, T. (2015). The Influence of Board of Director's Risk Oversight on Risk Management Maturity and Firm Risk-Taking. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2482791

Khan, H. (2011, December). A Literature Review of Corporate Governance. In *International Conference on E-Business, Management and Economics* (Vol. 25, pp. 1-5). IACSIT Press.

Kumar, A. S., & Sable, A. (2022). Corporate Governance and Risk Management. Part 2. *Indian Journal of Integrated Research in Law, 2,* 1.

Li, W. A., Hao, C., Cui, G. Y., Zheng, M. N., & Meng, Q. K. (2019). Forty Years of Corporate Governance Research: A Review and Agenda. *Foreign Economics & Management, 12,* 161-185. https://doi.org/10.16538/j.cnki.fem.2019.12.008

Lundqvist, S. A. (2015). Why Firms Implement Risk Governance—Stepping beyond Traditional Risk Management to Enterprise Risk Management. *Journal of Accounting and Public Policy, 34,* 441-466. https://doi.org/10.1016/j.jaccpubpol.2015.05.002

Oterholm, T. R. (2024). *Risk Appetite on a Strategic and Operational Level*. Master's Thesis, NTNU.

Passaris, C. E. (2006). The Business of Globalization and the Globalization of Business. *Journal of Comparative International Management, 9,* 3-18.

PWC (2011). *In Times of Uncertainty—An Insight into Effective Risk Reporting in a Changing Market*. https://www.pwc.com.au/industry/banking-capital-markets/assets/insight-into-effective-risk-reporting-sep11.pdf

Renn, O. (2008). *Risk Governance. Coping with Uncertainty in a Complex World*. Earthscan.

Stein, V., Wiedemann, A., & Bouten, C. (2019). Framing Risk Governance. *Management Research Review, 42,* 1224-1242.

Wu, J., & Wu, Z. (2014). Integrated Risk Management and Product Innovation in China: The Moderating Role of Board of Directors. *Technovation, 34,* 466-476. https://doi.org/10.1016/j.technovation.2013.11.006