RISK MANAGEMENT AND CORPORATE GOVERNANCE

Interconnections in Law, Accounting and Tax

EDITED BY

Marijn van Daelen • Christoph Van der Elst

Risk Management and Corporate Governance

Interconnections in Law, Accounting and Tax

Edited by

Marijn van Daelen

Tilburg University, The Netherlands

Christoph Van der Elst

Tilburg University, The Netherlands
Ghent University, Belgium

Edward Elgar

Cheltenham, UK • Northampton, MA, USA

Published by
Edward Elgar Publishing Limited
The Lypiatts
15 Lansdown Road
Cheltenham
Glos GL50 2JA
UK

Edward Elgar Publishing, Inc.
William Pratt House
9 Dewey Court
Northampton
Massachusetts 01060
USA

A catalogue record for this book
is available from the British Library

Library of Congress Control Number: 2010926008

ISBN 978 1 84980 395 3

Printed and bound by MPG Books Group, UK

Contributors

Filip Bogaert
Filip Bogaert was admitted to the Bar of Ghent in 2002. In 2006 he also became a member of the Financial Law Institute of the Ghent University (Belgium). His research focuses on credit risk, credit risk transfer, credit derivatives and securitization. At present he's preparing a Ph.D. in law about credit risk and credit risk transfer.

Marijn van Daelen
Marijn van Daelen has been a research fellow and lecturer at Tilburg University Faculty of Law (Netherlands) since 2006. Her research focuses on business-law-related topics, such as corporate law, corporate governance, disclosure, risk management, internal control and compliance. Currently she is preparing a Ph.D., which analyses risk management and internal control from a legal perspective. Moreover, she works on several research projects related to the above subjects.

Christoph Van der Elst
Christoph Van der Elst is Professor of Business Law and Economics at the Law School of the University of Tilburg (The Netherlands). He combines this position with a professorship at the Law School of the Ghent University (Belgium). He is also a member of the disciplinary court for the Belgian registered auditors. He holds a Master degree in Law, a Master degree in Economics and a Ph.D. in economics. His research interests primarily concern different issues of corporate governance, corporate risk management and company law and, in particular, the position of shareholders in the law and finance theory.

Ronald Russo
Ronald Russo has been a researcher and lecturer at the Fiscal Institute of Tilburg University (Netherlands) since 2006. Prior to this he worked for the universities of Utrecht and Leiden, combining this with his work as a tax inspector and tax consultant. His holds a Ph.D. in (tax) law (1992). His current research includes the concept of profit for taxation purposes and the interactions with profit for commercial purposes, nationally but also in a European perspective.

Arco van de Ven

Arco van de Ven is Professor of Accounting Information Systems at TiasNimbas, the business school of Tilburg University and Eindhoven University of Technology. He is a registered auditor (Register Accountant), the Dutch equivalent of a Certified Public Auditor (CPA) and received his Ph.D. at Erasmus University Rotterdam, where he has also been programme director of the following courses: the postgraduate Executive Master of Finance and Control (Dutch: register controller RC); and the postgraduate Master Certified Public Controlling (CPC). He has also taught various post-experience programmes at Vlerick Leuven Gent Management School. Professor Van de Ven is also a partner at ACN Management Consultants and has performed many (interim) functions as CFO, controller and consultant.

Foreword

How much risk is a company involved in and how does it manage these risks? These questions have probably been raised more often over the last couple of years than any other business-related question. Risk management is high on the agenda of legislators, governments, supervisors, consultants and, not least of all, companies, not only in the financial sector, but also in many other businesses as well. The stakeholders and shareholders also have huge expectations regarding the proper disclosure of risk management. It poses other risks of which the appropriate balance between (1) the necessary disclosure of risks and (2) the appropriate confidentiality of some business activities is the most important one. It raises important questions such as which types of transparency, standardization and attestation rules can reduce the risk of misappropriation of corporate funds, misstatement of financial reports and can also mitigate the engagement in too-risky strategies. The processes and procedures that are developed both at the regulatory level as well as at the corporate level should take into account standardization of the internal control and risk management systems. Moreover the disclosure of these elements could overemphasize the actual risk and crowd out the agility of organizations and the entrepreneurial spirit needed for the continuity of the organizations and companies. Procedures to standardize the disclosure of internal control and risk management systems are in place. A recent interesting example of this development is the 'High Level Principles for Risk Management' of the Committee of European Banking Supervisors of February 2010. Further, transparency, standardization and attestation rules need to be approached in an integrated way: disclosure of information has not always led to increased transparency and requires content standardization for which appropriated control mechanisms, that is, attestation rules are necessary.

In different disciplines risks and risk management systems are approached in a uni-dimensional way. However, companies are confronted with risks at many different levels and in many layers inside and outside the business: strategic or generic risks, operational risks, financial risks and legal risks and risk management systems that must be able to cope with all these different kinds of threats. It requires a more holistic approach. This book provides the initial impetus for a more interdisciplinary approach. The authors give a comprehensive overview of historical and current provisions relating to internal control and risk management in Europe and the US. Next, the interconnected consequences of the necessity of risk management (the risk management landscape) are addressed. It shows that a comprehensive approach (accounting, business law, financial law and tax law) needs to be further improved. In different fields of practice and in particular, in accounting, an expectation gap is visible: users of services expect that the services are always reliable and cannot contain any errors, while information systems and control frameworks increase the reliability and reduce the probability of fraud and failure, but it remains impossible to provide 'hard' control guarantees. The answer to the gap lies, *inter alia*, in the requirement to deliver the best audit quality possible. The public expects auditors to detect all fraudulent behavior and auditors do not accept responsibility for this level of fraud detection. Risk management is an integrative part of the general framework to increase the likelihood of reliable procedures, operations and (financial) information, including tax management. The latter requires the fulfillment of all formal tax duties and the appropriate record of the amounts of taxes payable in commercial accounts.

Many of the aforementioned topics are addressed in this book. It will serve the discussion to further develop the integrative academic analysis of risks and risk management systems. The last chapter provides the authors' valuable insights about how to proceed. Reading between the lines, it is clear that they support a more principle-based approach of both accounting standards and the accompanying risk-management approach. Based on an analysis of the pros and cons of both the rule-based and the principle-based approach, the book shows that the latter makes it more feasible that sound business practices can be combined with the strategic goals of the company and the relationship between entrepreneurial risk taking and sound risk governance management is in equilibrium. It will also necessitate a balanced supervision framework that both prevents excessive risk taking *ex ante* and addresses risk failures *ex post*. Enjoy reading!

André Kilesse
Vice President
Federation of European Accountants

Acknowledgments

This book arose out of the idea that academics in different fields were addressing the developments and state-of-the-art of the risk management environment in which corporations operate. All authors responded enthusiastically to the request to cooperate and provided insights in their different contributions. We would like to thank these authors for sharing their views and providing us with their latest work in this field.

We also want to thank Arco for his professionalism and support of this project. We owe a large debt of gratitude to Kim Raaijmakers for her excellent editing assistance. We are also grateful to COSO, managed by AICPA as well as Ericsson for providing the right to publish the 'cubes' and an excerpt from the annual report.

We have benefitted from the valuable insights that practitioners provide to our students in the law and management master programme. We would like to thank them for their inspiring lectures. Finally, we would like to thank the University of Tilburg and, in particular, the department of business law for its stimulating research environment.

Tilburg, February 2010.

Marijn van Daelen
Christoph Van der Elst

Contents

Figures, tables and boxes

FIGURES

TABLES

BOXES

1. Introducing risk management

Marijn van Daelen and Arco van de Ven

1.1 INTRODUCTION

In reaction to the recent financial crisis and the corporate failures and frauds at the beginning of the millennium, the emphasis of the business community in corporate governance has shifted towards internal control and risk management issues. This shift has not only been fuelled by fraud but also by excessive directors' remunerations, growing internationalisation, inadequate reporting, failing auditors and – especially in recent years – the development of complex financial instruments and their associated risks. Although risk management is not a new feature of businesses and corporate governance, it is currently high on the corporate agenda. Risk management discussions were never of this magnitude before, either among academics, policymakers, lawmakers or practitioners.

This book provides a comprehensive approach in accounting, and business, financial and tax law to risk management. These fields are all interrelated and describe and require particular behaviour within organizations. Chapters 2 to 5 provide an elaborate account of the development of risk management at EU level, within some EU member states and in the USA. These chapters explore relevant current risk management discussions and reforms in order to address possible future directions. Chapter 2 deals with risk management from an accounting perspective and Chapter 3 addresses risk management from a business law perspective. Chapter 4 analyses risk management in financial law and Chapter 5 describes risk management in taxation. Finally, Chapter 6 paints the overall risk management landscape in order to show the interconnections between the developments in law, accounting and tax. Some of the developments in these areas do not stand on their own but are (knowingly or unknowingly) influenced by developments in the other disciplines. Other developments are a reaction to irregularities on markets or in companies and do not take account of the developments in other disciplines. Chapter 6 concludes with some challenges and problem areas that risk management faces. The international and multidisciplinary approach of this final chapter gives an insight into the overall influence of risk management on companies and on society as a whole, taking the corporate governance discussion to a higher level. In general, all chapters focus on listed companies because internal control and risk management reforms specifically address publicly held companies, although the reforms also affect non-listed companies and government governance. To start off, this chapter will briefly discuss the concept of risk management, as well as some leading definitions.

1.2 THE CONCEPT OF RISK MANAGEMENT

According to Beck today's society is a risk society.[1] Modernity is characterized as and influenced by a *risk management discourse*. Decisions can apparently only be taken after a thorough risk analysis. Companies need a business control, an accounting control and a tax control framework to survive and risk management has become an important corporate governance issue. To many people risk has become ubiquitous[2] and it seems as if a risk-based description of everything is pivotal.[3] Risk is not to be seen as an act of providence, but as a potential event that can be measured and managed.

The struggle to master risks is one of all times. The ancient Greeks prayed to their gods to protect them on their journeys and in their wars. Peter Bernstein[4] wrote a book on the story of risk: *Against the Gods*. In it, he describes the development of risk management as a process of man being liberated from oracles and soothsayers and taking the management of risk into his own hands. The law of probabilities defined by Fermat and Pascal in 1654 was a first important step in this process. The outcome of a game of chance was no longer just a belief. Risks could be seen as probabilities and could even be calculated. The transition from a game of chance to natural events was soon made. In a book published in 1662 the probability of being struck by lightning was compared with the intensity of people's fear of thunder. The author concluded that given the slight possibility of such an event occurring, people's fear was too strong and that fear ought to be proportional to the gravity of the harm and the probability of the event.[5] Today, risk management systems are still based on these two pillars: probability and gravity.

---

1 Beck 1992.
2 Hood, Jones, Pidgeon, Turner, Gibson et al. 1992, p. 135.
3 Power 2004, p. 2.
4 Bernstein 1996.
5 Bernstein 1996, p. 71.

The possibility of predicting probabilities increased when in 1733 the French mathematician Abraham de Moivre revealed his normal-distribution formula, also known as the bell curve. Observations far from the mean are less frequent than observations close to the mean and when plotted are bell-shaped. With this formula it could be determined whether a set of observations represented the universe of which they are a part, making statistical predictions possible without measuring all possible events. Forecasting probabilities has since moved on from natural events such as lightning to virtually all elements of life. For instance, life insurance premiums can be calculated on the basis of mortality statistics.

A model presented by Black and Scholes[6] made it possible to calculate the value of options. The ramifications of this technique were mind-boggling. Valuation of all kinds of complex financial products was now attainable. For example, only a few people expected that it would be possible to sell football tickets for future matches of Arsenal Football Club, but this is exactly what Arsenal did in 2006: it sold the future revenue of tickets for £260 million.[7] Ticket sales and ticket value no longer depend on uncertain events such as coach tactics, player transfers, injuries or missed penalties. To a large extent they can be predicted, calculated and valued up front.

The journey from being passive prisoners of providence, who felt they could not but resign themselves to submitting to all risks that life threw at them, to independent actors, who think that all possible events can be measured (and sold) in advance, has been a long one. With the increased possibilities to manage risks has come the unprecedented rise in hazards and potential threats. Welcome to the risk society![8] This is the society where most are stakeholders who depend on how organizations manage their risks. For example, consumers rely on the quality of the food they buy, shareholders face the risks of losing their investments, and employees depend on pension funds for their retirement benefits. Moreover, society as a whole is exposed to a broad range of hazards that may cause irreversible harm, ranging from radioactivity and global warming to pollution. History shows that these risks unfortunately are very real. Next to bad management caused by incompetence, economic theory predicts opportunistic behaviour or self-interest-seeking with guile, which refers to 'incomplete or distorted disclosure of information, especially to calculated

---

6 Black & Scholes 1973.
7 Euromoney 2006.
8 Beck 1992.

efforts to mislead, distort, disguise, obfuscate, or otherwise confuse'.[9] History abounds with examples of poor governance.[10] Different types of standards and codes have been developed over the years to describe, measure and report on varied risk-related items. Different accounting and auditing standards as well as business, financial and tax laws and corporate governance codes describe and sometimes prescribe behaviour within organizations. There is an evolving trust in numbers and standards as a basis for rational decision making.[11]

1.3 LEADING DEFINITIONS

Before describing the development of risk management in the following chapters, this chapter will first give some of the leading definitions of risk and risk management. To begin with, risk from an organizational perspective is often seen as 'a threat to an organization that reduces the likelihood that the organization will achieve one or more of its objectives'.[12] This definition limits risk to the negative aspects of possible events. The International Standards Organization (ISO) also includes the positive impacts of events in its definition: 'risk is the effect of uncertainty on objectives'.[13]

Risk is often distinguished from uncertainty,[14] because of the difference between the incalculability of uncertainties and the calculable nature of risks based on the availability of probabilistic knowledge. Power declines this view,[15] arguing that practitioners of risk management do not differentiate between risk and uncertainty on these grounds. Risks and uncertainties are not two different classes of *objects*. Uncertainties become risks as soon as they enter the management domain. He draws on the notions of Luhmann that the concept of risk itself implies these dangers have entered the domain for decision making, where responsibilities for these dangers are allocated. Positioning risk in the management domain means that risks are perceived as being open not only to analysis, but also to systematic management. The practice of risk management is thus transformed from risk analysis into an organizational process with a standard set of perform-

---

9 Williamson 1985, p. 47.
10 See e.g. Skeel 2005.
11 Power 2007, p. 13.
12 Knechel 2001, p. 26.
13 ISO 2009, p. V.
14 Knight 2006, p. 20.
15 Power 2007, p. 5.

ance activities for risk management, the business control frameworks. The leading framework of enterprise risk management is given in the COSO II Report, which defines Enterprise Risk Management as [16]

> [. . .] 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.[17]

Risk management cannot deliver absolute certainty. *Reasonable assurance* reflects the notion that uncertainty and risk relate to the future, which no one can predict with precision.[18] Yet *reasonable* does not imply that enterprise risk management will frequently fail.[19] *Risk appetite* is defined as 'the amount of risk, on a broad level, an entity is willing to accept in pursuit of value'.[20]

Enterprise risk management as defined by COSO II is a broad and all-encompassing concept. The objective of risk management includes the objectives of internal control, which is the process within an organization to achieve reasonable assurance of effectiveness and efficiency of operations, reliable reports, compliance with applicable laws and regulations and of safeguarding the organization's assets against misappropriation (fraud). In addition to internal control, enterprise risk management is aimed at the strategic control of an organization. From a corporate governance perspective the purpose of effective risk management could be aimed at different types of risks, ranging from fraud and embezzlement to financial shenanigans,[21] mismanagement or a perilous strategy.

REFERENCES

Beck, Ulrich (1992), *Risk Society – Towards a New Modernity*, London: Sage Publications.

Bernstein, Peter L. (1996), *Against The Gods*, New York: John Wiley & Sons.

Black, F. and M. Scholes (1973), 'The Pricing of Options and Corporate Liabilities', *Journal of Political Economy*, **81**, pp. 637–54.

---

[16] COSO 2004, p. 2.

[17] © COSO.

[18] COSO 2004, p. 20.

[19] COSO 2004, p. 20.

[20] COSO 2004, p. 19.

[21] Financial shenanigans are actions that intentionally distort a company's reported financial performance and financial condition. Schilit 2002, p. 24.

Euromoney (2006), 'Football Securitization: Arsenal kicks off public ticket receivables deals', available at http://www.euromoney.com/Article/1050208/BackIssue/50151/Football-Securitization-Arsenal-kicks-off-public-ticket-receivables-deals.html?Type=BackIssueArticle&ArticleId=1050208&ID=50151 (accessed 10 February 2010).

Hood, Christopher, David Jones, Nick Pidgeon, Barry Turner, Rose Gibson, et al. (1992), *Risk Management* in The Royal Society *Risk: Analysis, Perception and Management,* London: The Royal Society.

Knechel, Robert, (2001), *Auditing, Assurance & Risk*, Cincinnati, Ohio: South-Western College Publishing.

Knight, Frank H. (2006), *Risk, Uncertainty and Profit*, New York: Dover Publications inc.

Power, Michael (2004), *The Audit Explosion,* London: Demos, available at: http://www.demos.co.uk/files/theauditexplosion.pdf?1240939425 (accessed 8 February 2010).

Power, Michael (2007), *Organized Uncertainty – Designing a World of Risk Management*, Oxford: Oxford University Press.

Schilit, Howard M. (2002), *Financial Shenanigans – How to Detect Accounting Gimmicks & Fraud in Financial Reports – 2nd edition*, New York: McGraw Hill.

Skeel, David A. (2005), *Icarus in the Boardroom: The Fundamental Flaws in Corporate America and Where They Came From*, New York: Oxford University Press.

Williamson, Oliver E. (1985), *The Economic Institutions of Capitalism*, New York: The Free Press.

CODES AND GUIDELINES

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004), *Enterprise Risk Management – Integrated Framework*, Executive Summary, New York: AICPA Inc., (COSO II Report).

International Standard Organization (ISO) (2009), *31000: 2009 Risk management – Principles and guidelines*, Geneva: ISO.