Vinay Kalia
Roland Müller
Editors

Risk Management at Board Level

A Practical Guide for Board Members

3rd edition

HAUPT VERLAG

For my beautiful and loving daughter Vinaya Melania
Vinay Kalia

For my unique and supportive wife Barbara
Roland Müller

3. Auflage: 2019
2. Auflage: 2015
1. Auflage: 2007

Bibliografische Information der *Deutschen Nationalbibliothek*
Die Deutsche Nationalbibliothek verzeichnet diese Publikation
in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet
über http://dnb.dnb.de abrufbar.

ISBN 978-3-258-08124-3

Satz und Layout: Die Werkstatt Medien-Produktion GmbH, D-Göttingen

Printed in Austria
www.haupt.ch

Foreword by the Editor of this Series

Professor Martin Hilb

Board of Directors (BoD) effectiveness is currently one of the few subjects that are topical for both research and practice globally. In this series, our International Center for Corporate Governance presents the results of studies conducted by its partners.

Our approach to Board of Directors (BoD) effectiveness is based on the following guiding principles:

- Keep it situational;
- Keep it strategic;
- Keep it integrated;
- Keep it controlled.

This edition, presented by our two partners Dr.oec. HSG Vinay Kalia (who wrote his doctoral thesis on the subject of Risk Management on the Board of Directors (BoD) and Executive Board (ExB) level under my supervision) and Prof. Dr.iur. Roland Müller fits into the last principle, «keep it controlled».

Keeping it controlled includes auditing, Risk Management, communication, compliance and evaluation on the Board of Directors (BoD) level.

One result of the Board evaluations we conducted in many organisations is that Risk Management on the board level is an area for development.

A single error alone never lets a company collapse. The cause often lies in the lack of an effective and systematic Risk Management function at the Board of Directors (BoD) level. It should be noted that:

- The new phase in Risk Management started in the 1970s with the growth of credit Risk Management;
- The Risk Management approach in the 21st century takes a holistic view of all risks concerning a company;
- The New York Stock Exchange (NYSE), through its Securities Exchange Commission (SEC), sponsored legislation such as the Sarbanes Oxley Act

(SOX) to put additional and mandatory pressure on companies to manage risks on the operational and Board of Directors (BoD) levels and provide totally transparent information to shareholders;

- The financial crisis of 2008 triggered regulatory developments (Mifid, FATCA etc.) that have reinforced the need for and interest in Risk Management and its importance will continue to increase in the foreseeable future;
- Essentially, small and medium companies (SMEs) and very small companies feel that Risk Management does not have any meaning for them. However, Risk Management can be implemented even in such companies both on operational and Board of Directors (BoD) levels with great effectiveness and added value for the company.

Effective Boards need both: Members with profound entrepreneurial spirit and Risk Management know-how. This will decide if companies are the masters or victims of change.

St. Gallen/ Switzerland, January 2019

Martin Hilb
Chairman of the Board Foundation (www.icfcg.org) and
its Swiss Board School at the IMP of the University of St. Gallen

Foreword by the Authors

Dr.oec. HSG Vinay Kalia
Prof. Dr.iur. Roland Müller

In the last few years, the world has been transformed by a string of developments which have raised the risk awareness and have moved Risk Management into the centre of attention, at the governance level of all corporations, regulators, public sector institutions and non-governmental organisations. Some of those developments need to be highlighted:

- The major financial crisis of 2008 sparked off many discussions about governance and control of operational risk in financial institutions, like the «too big to fail» discussion. These discussions were intensified by an increasing interest and control stake on the part of the regulators, which is often being criticised as «over-regulation». In the past, internal control systems and compliance activities focussed mainly on financial and legal issues, whereas now they also encompass other risks such as IT security or fraud risks, in order to provide senior decision makers with appropriate risk data;
- Black Swan events such as large scale cyber threats, war, nuclear or natural catastrophes have become more frequent and devastating, even more so as the world has become increasingly interdependent and complex. Such Black Swan events bear unforeseeable and uncontrollable risks. This has substantiated the need for organisations to be prepared for risk, to be «resilient» and focused on Business Continuity Management (BCM);
- Social risks such as the demographical development, migration, religious and national conflicts or resource allocation now directly affect the businesses and their response to such issues, accentuated by the ethical and cultural diversity;
- Large firms have several projects ongoing that are large enough to be firms on their own, either in terms of size or complexity. Thus a lot is at stake financially and existentially for the firm («trillion is the new billion»).

These firms have increasingly felt the need for project Risk Management as it enables both self-governed process management and information escalation.

The above illustrates that Risk Management has in the last years become even more important than before and many formal and material changes have occurred.

Our objective for the first edition of this book was to present readers with a practical understanding of risk and Risk Management, with all its facets and topics, providing real life examples, tools, guidelines and checklists to manage them.

The book has been used and appreciated by practitioners, especially by board and senior management members who participated in board governance seminars. This because the developments discussed above are on their minds and agendas very often. Their questions raised to the authors and the discussions resulting from them have been reflected in the second edition. Moreover, all context and contents of the book have been updated. Further thought has been given to the discussion of Risk Management as a «system» rather than theme, to Compliance, Internal Controls (section II.3) and to the establishment of the right Risk Management culture (IV.9).

To complement and reflect on the emerging Risk Management needs for today, three guest authors were invited to enrich the book with their subject matter expertise.

- Lee Howell, presents in chapter V how the phenomenon of uncontrollable risks and black swan events can be understood and practically managed by firms;
- Peter Jonker, in chapter VI, explains why fraud and corruption risks are different from all other risk categories and what is required to keep the firm away from serious risks and damage related to them;
- Stephan Döhler, in chapter VII, sheds light on the project Risk Management where the success of big or vital projects has a significant influence on the health and wellbeing of the firm.

A special word of thanks to them for sharing their experience and thoughts. Special thanks to Mark Macus for reviewing the first edition of the book and providing valuable inputs for improving and updating the new edition. Finally, we highly appreciate Martina Schedler and Beat Gyger for working tirelessly in providing the final shape to the manuscript.

It is our sincere hope that this book benefits readers, especially Directors of the Board as well as Executive Managers, in embracing the new risk landscape and empower them with the help of a practical tool-kit to create a systematic and effective Risk Management.

St. Gallen / Switzerland, January 2019 Vinay Kalia / Roland Müller

Table of Contents