

**Vinay Kalia
Roland Müller
Editors**

Risk Management at Board Level

A Practical Guide for Board Members

HAUPT VERLAG

For my beautiful and loving daughter Vinaya Melania
Vinay Kalia

For my unique and supportive wife Barbara
Roland Müller

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 978-3-258-07896-0

Alle Rechte vorbehalten.

Copyright © 2007 Haupt Bern

Jede Art der Vervielfältigung ohne Genehmigung des Verlages ist unzulässig.

Printed in Austria

www.haupt.ch

Table of Contents

Foreword by the Editor of this Series 5

Foreword by the Authors 7

Table of Contents. 11

Abbreviations 21

I. Introduction 25

1. General Overview 25

2. Importance of Risk Management 28

 a) Help for Company 28

 b) Bank Rating.....28

 c) Insurance.....28

3. Role of Board Members in Risk Management. 29

 a) Risk Management as a Part of Good Corporate Governance .29

 b) 360° Direction and Control.....30

 c) Setting the Tone of Risk Management 32

 d) Dealing Effectively with Strategic Issues.....32

 e) Fostering Openness and Creativity.....33

 f) Guidelines and Policies for Risk Management.....33

 g) Serious and Extraordinary Decisions 34

 h) Supervision of the Company Performance Versus Strategy .34

 i) Organisation and Structure of Risk Management.....34

4. Definitions and Concepts 37

 a) Definition of Risk and Security.....37

 b) Definition of Risk Controlling 39

 c) Definition of Risk Management 39

 d) Definition of Emergency Management 40

 e) Definition of Crisis Management 40

 f) Definition of Operational Risk Management 41

 g) Concept of Value-at-Risk.....41

 h) Concept of a Risk Map.....43

 i) Concept of Business Continuity Management (BCM).....44

5. Risk Management Standards.	47
a) Committee of Sponsoring Organisations (COSO) Framework	47
b) Sarbanes Oxley Act 2002	49
c) ISO 31000 & 31010 (Risk Management & Risk Assessment) ..	51
d) ISO 19600 (Compliance)	53
II. Development of Risk Management	56
1. Overview of the Development Stages.	56
2. Risk Management and Corporate Governance.	60
a) Overview of ERM and Corporate Governance Interdependence	60
b) The Cadbury Report.	62
c) The Combined Code and Hampel Report	63
d) The Turnbull Report	63
e) The King II & King III Reports	65
f) The Basel Committee Reports	66
3. Risk Compliance	67
a) Establishing of the Compliance Function at the Executive Level	68
b) Guidelines for Compliance Management System	70
c) Elements of a Compliance Management System (CMS)	70
III. Driving Forces of Risk Management in Switzerland.	73
1. General Overview	73
2. Law as a Driving Force	74
a) Importance of Several Regulations	74
b) Swiss Code of Obligations	75
c) Bank Regulations	75
d) German Law for Control and Transparency (KonTraG).	76
3. Institutional Investors	76
4. Impact of US Developments	77
5. Press	77
6. Others	78

IV. Risk Management Implementation	79
1. General Overview	79
2. Objective Setting	82
a) SWOT-Analysis	82
b) Risk Management Policy	82
c) Risk Management Guidelines/ Directives	84
d) Risk Management Handbook	84
3. Risk Identification	84
4. Risk Assessment and Prioritisation	87
5. Risk Analysis	91
a) Key Drivers Analysis/ Root Cause Analysis	92
b) Suitable Actions to Respond to the Key Drivers	93
6. In-depth Risk Analysis	96
a) Quantification of Risks	96
7. Action Planning	97
8. Monitoring, Reporting and Supervision	98
9. Culture	104
10. Tools	107
11. Timeline and Cost of Risk Management Implementation	108
V. Uncontrollable Risks and Corporate Governance	111
1. Defining Uncontrollable Risks	111
a) Complicated Systems	113
b) Complex Systems	113
2. Complex Systems Shaping Current Economic Landscape	113
3. Era of Black Swan Events (BSE)	116
4. Uncontrollable Risks and Boards	117
VI. Managing Fraud and Corruption Risks	125
1. Problem Overview	125
a) Clarity of Norms	126
b) Risk of Being Caught	126
c) Difficulty to Discuss	127
d) Intentional Act	129

2.	Who are Involved?	129
a)	Red Flags	130
b)	Departments Involved in Fraud Cases	131
3.	Common Forms of Corruption	133
a)	Gifts and Entertainment	133
b)	Facilitation Payments and Bribes	133
c)	Kick-backs and Overbilling Schemes	133
d)	Bid-rigging and Price Fixing	136
e)	Use of Agents.....	136
f)	Political Support and Charitable Contributions	136
4.	Managing the Risk of Fraud and Corruption	137
a)	Effective Compliance Programs	138
VII.	Risk Management of Major Projects	141
1.	Why Risk Management of Projects at Board Level?	141
2.	Risk Management Guidelines	143
3.	Project Management Handbook.	146
4.	Project Credit Demand Report to the Board of Directors	146
5.	Final Major Project Credit Demand Report (Closing of Internal Credit Line)	149
6.	Reporting of Major Projects to the Board of Directors (Guidelines)	150
a)	Definition of a Major Project	150
b)	Standard Major Project Report to the Board of Directors ...	152
7.	Aggregated Risks of a Company in Relation to Major Projects.	155
a)	Group Risk Report to the Board of Directors	156
b)	Risk Inventory.....	156
c)	Risk Inventory for Major Projects.....	156
8.	Communication in Major Projects.	157
9.	External Risks for Major Projects	158
10.	Decision-making to Minimise or Mitigate Risk of Major Projects.	160

VIII. Summary and Guidance for Practice	162
1. Summary	162
a) Key Messages	162
b) Organisation at Board Level	163
c) Organisation at the Management Level	163
d) Risk Management in the Company	164
e) Managing Uncontrollable Risks	164
f) Managing Fraud and Corruption Risk	165
g) Risk Management of Major Projects	165
2. Risk Management Practice Today	166
a) Integrated ERM	166
b) Decision-Making Under Time Pressure	168
c) Whistleblowing	169
d) Checklists	169
e) Small and Medium Companies	170
f) Managing Impediments	171
g) Self-Appraisal	173
h) Keep it Simple	173
Epilogue	175
Bibliography	176
Appendices	181
Editors	234

List of Appendices

Appendix 1: Checklist for Implementing Enterprise Risk Management	.182
Appendix 2: Example of a Risk Management Policy	184
Appendix 3: Example of Internal Regulations for Risk Committee	197
Appendix 4: Example of a Risk Identification Form	200
Appendix 5: Questionnaire for IT Risks	202
Appendix 6: Example of a Whistleblowing Policy Document	204
Appendix 7: ERM Self-Appraisal Questionnaire	208
Appendix 8: Guidance for FO ² RDEC Analysis	212
Appendix 9: Job Description for Head of Risk Management/ CRO	215
Appendix 10: Example of an Individual Risk Assessment	217
Appendix 11: Insurance Check List for BoD	220
Appendix 12: Generic Collection of Master Risks	222
Appendix 13: Scenarios of the RESIST Methodology	223
Appendix 14: Examples of Anti-Corruption Controls	225
Appendix 15: Practical Guidance for the BoD on Uncontrollable Risks	..229
Appendix 16: Elements of a Code of Conduct	233

List of Figures

Figure 1: Corporate Risk Management (CRM) Framework.....	27
Figure 2: 360° Overview by Risk Radar.....	31
Figure 3: Risk and Security.....	38
Figure 4: Four Main Types of Risk	38
Figure 5: EBIT@RISK Concept	42
Figure 6: The Classical Risk Map.....	42
Figure 7: Example of a Risk Map.....	44
Figure 8: Business Continuity Management Umbrella	46
Figure 9: COSO Enterprise Risk Management Framework	48
Figure 10: Relationship Between Principles, Framework and Process....	52
Figure 11: Flowchart of a Compliance Management System	55
Figure 12: Evolution of Risk Management.....	59
Figure 13: Spiral Approach to Risk Management at Board Level.....	61
Figure 14: Governance, Risk and Compliance Management System (GRC)	68
Figure 15: Relationship Between Various Risk Management Processes....	72
Figure 16: Forces Fostering Better Risk Management in Switzerland	78
Figure 17: ERM Conceptual Framework	80
Figure 18: Risk Classification.....	86
Figure 19: FMEA Works at All Levels	87
Figure 20: Risks Listed Based on FMEA Workshop.....	89
Figure 21: Risk Map	90
Figure 22: Example of a Key Driver/ Root-cause Analysis	92
Figure 23: Measures Listed Based on FMEA Workshop	94
Figure 24: Measure Matrix.....	95
Figure 25: Risks Gradually Reduce	97
Figure 26: Key Strategies to Manage Risks	98
Figure 27: Example of a Periodic Trend Analysis.....	101
Figure 28: ERM Implementation Overview	103
Figure 29: Globalisation and Systemic Risk	112
Figure 30: Natural Disasters & Technological Disasters Events	115
Figure 31: Turning Black Swans into White Swans	118
Figure 32: Interconnectedness of Main Risks.....	121

Figure 33: Interconnectedness of Specific Risks.....	122
Figure 34: Occurrence of Code of Conduct Violations.....	128
Figure 35: The Fraud Triangle.....	129
Figure 36: Behavioral Red Flags Displayed by Perpetrators	131
Figure 37: Departments Most Likely Involved in Non-Compliance Cases	132
Figure 38: The Fraud Tree	134
Figure 39: Elements of Fraud Risk Management Framework.....	138
Figure 40: Impact of Hotlines	140
Figure 41: Risk Reporting Line of a Major Project	145
Figure 42: Reporting Line of a Credit Demand Report for a Major Project	147
Figure 43: Example of the Organisational Structure of a Major Project ..	151
Figure 44: Organisation of a Standard Major Project Report (Reporting Line)	154
Figure 45: The Global Risks Landscape 2013.....	159
Figure 46: Integrated Risk Management.....	167
Figure 47: Perrow's Dilemma in Management.....	174

List of Tables

Table 1: Mistakes and Deficiencies at Board Level 29

Table 2: Overview of Common Constructs of Risks. 37

Table 3: Timeline of Risk Management Implementation.....108

Table 4: Costs of Implementation of Risk Management Year 1 109

Table 5: Costs of Implementation of Risk Management after Year 1 109

Table 6: Black Swan Event Theory 117

Table 7: Two Frameworks for Studying Human Error 119

Table 8: Essentials of Enterprise Risk Management for Different
Scale Companies 170

I. Introduction

1. General Overview

Risk Management is not a new idea or concept. There were forms of Risk Management at all times and for all kinds of scenarios that had to be managed by man. Risk Management implies that actions are taken to anticipate, minimise or mitigate risks from imminent or future events, with the goal to master and control them.

In an enterprise quite a number of individuals work together. This circumstance creates not only a common goal and interest but also a shared destiny and shared risks, which again leads to a need for increased control to manage such risks. The performance of an enterprise has direct or indirect effects not only on the employees but also on the owners (shareholders), customers, suppliers, and other stakeholders. And in turn that network of interest groups also influences the company, which bears additional risks. Therefore, a company must be aware of all such mutual impacts and risks. It is held accountable and expected to take corresponding actions.

Collecting and systematically analysing its risks and measures taken to handle them may be called the process of Risk Management, or just simply Risk Management. Complex and wide-ranging as it may have become, Risk Management is not meant to be a bureaucratic and control-focused exercise in its own right. It should be an integrated yet all-embracing process that increases awareness, understanding and handling of impacts and risks in and around the company. Not least to increase certainty and reliability of the future for a large number of individuals, especially in times of volatility and instability. It goes without saying that not only big companies but also medium and even small firms need Risk Management, though the depth of analysis, formality of processes, organisation and resource allocation may vary according to size, complexity and risk exposure in a given business.

Risks are all around and well known to many and yet they are often recognised as such too late, so that neither enough time nor adequate measures

are available to prevent them from materialising in their full potential or to minimise the damage for the company. A good top management should aim to recognise risks at an early stage and should try to minimise the most dangerous amongst them through adequate strategic or tactical measures. Consciously or unconsciously every enterprise management pursues Risk Management but the endeavour should be to optimise the risk measures overall. Appendix 1 outlines an Enterprise Risk Management Implementation Check List. It provides a good overview of what Enterprise Risk Management entails and which key phases are involved in establishing organisation-wide in an effective and efficient way.

In article 716a of the Swiss Code of Obligation (CO) under number 1, the ultimate direction of the company is assigned to the BoD. In connection with these tasks, the BoD also has the untransferable and unalienable duty to avoid unnecessary risks and minimise inevitable risks in order to guarantee the existence and the advancement of the enterprise. Not surprisingly, since 2008 article 663b CO includes an obligation for all companies to comment on their risk assessment in the notes to the annual financial statement.

To be able to compare the efficiency of Risk Management between different companies, a certain standard is necessary with regard to the following points:

- Terminology with regard to the use of concepts;
- Risk Management implementation process;
- Organisational structure of Risk Management;
- Objective of Risk Management.

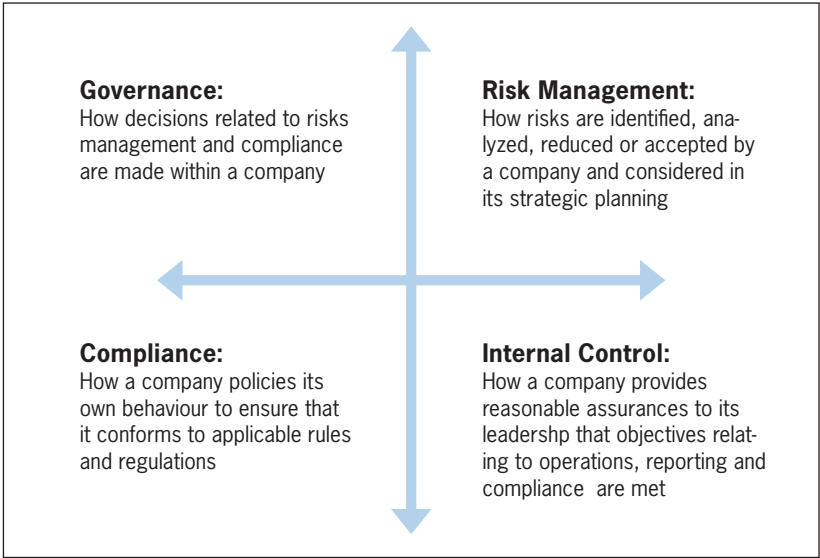
Such standards were introduced in the UK after comprehensive accounts on the subject by different professional associations such as the Institute for Risk Management (IRM), the Association of Insurance and Risk Managers (AIRMIC), and the National Forum for Risk Management in the Public Sector (ALARM). The Federation of European Risk Management Associations (FERMA) and other similar initiatives have tried hard to translate the standards into practice, so that organisations and enterprises could compete within this framework.

Governance, Risk Management and Compliance are increasingly referred to collectively as «GRC»¹, with the corporate functions being linked conceptually:

«Activist shareholders, institutional investors and policymakers look to these activities as crucial means for improving business ethics, enhancing the observation of legal norms, and deterring firms from engaging in unsafe or unsound practices. Regulators encourage companies to upgrade their activities in these areas; if companies do not comply, the regulators find ways to force them to do so.»²

The terms Enterprise Risk Management (ERM) and Corporate Risk Management (CRM) are often used interchangeably in research literature. Yet the use of the term «corporate» acknowledges the nexus between governance, Risk Management and compliance in a corporate context. (See Figure 1).

Figure 1: Corporate Risk Management (CRM) Framework

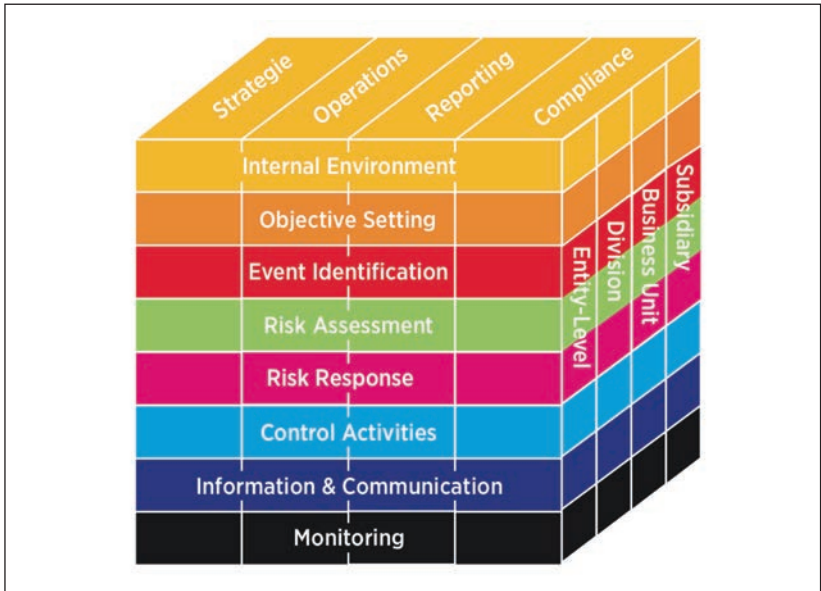


Source: Lee Howell

1 Miller (2014: 1).

2 Ibid.

Figure 9: COSO Enterprise Risk Management Framework



Source: COSO (The Committee of Sponsoring Organisations of the Treadway Commission) (2003)

ERM is considered to be a tool that adds value for companies and shareholders by:

- Aligning risk appetite and strategy;
- Enhancing risk response decisions;
- Reducing operational surprises and losses;
- Identifying and managing multiple and cross-enterprise risks;
- Improving deployment of capital.

COSO divides the entity's objectives into four categories: Strategic and operational objectives as well as Reporting and Compliance objectives. The activities to fulfil the objectives are carried out at all organisational levels such as the Enterprise/Corporate level, Divisional level, Business Units level and Subsidiary level. To guarantee that all different risks on all levels are handled in an equal way, a portfolio view of risks is recommended. This

means that management shares and conveys to all levels an entity-wide overview of risks and their co-relation. A risk framework may evolve from this. The ERM framework as shown in the figure above shows eight components.

The eight components do not materialise identically in every entity. Thus the framework may be less formal and less structured in small and mid-size entities than in large corporations. Nonetheless, small entities can have very effective Enterprise Risk Management, given all components are implemented and applied properly.

COSO claims that management be accountable to the board for all risks and their management, so that the board may be in a position to assume responsibility and provide governance, guidance and supervision. With the selection of the management, the board exerts great influence on values such as integrity or ethical attitude. It can assure its expectations are met through supervisory activities. Similarly, by reserving decision-making authority concerning specific key areas to itself, the Board of Directors (BoD) plays a role in mapping out strategy, formulating high-level objectives, and undertaking broad-based resource allocation. In terms of Enterprise Risk Management the board may exercise supervision by:

- Knowing the extent to which management has established effective Enterprise Risk Management in the organisation;
- Being aware of and concurring with, the entity's risk appetite;
- Reviewing the entity's portfolio view of risks and considering it against the defined risk appetite;
- Appraising the most significant risks and checking whether management is responding appropriately.

b) Sarbanes Oxley Act 2002

Sarbanes-Oxley Act (SOX), issued by the Public Company Accounting Oversight Board (PCAOB) in 2002, is in fact not a specific Risk Management framework or regulation. It is rather a regulation to improve internal controls and financial reporting. Signed into law by President George W. Bush in July

2003, the Sarbanes-Oxley legislation²⁵ turns the spotlight on Corporate Governance and aims to reduce the chances of another debacle like Enron.²⁶

What makes the law relevant for Risk Management relevant is the Sarbanes-Oxley Section 404: Assessment of internal control, which requires management and the external auditor to report on the adequacy of the company's internal control on financial reporting (ICFR).

Under Section 404 of the Act management is required to produce an «internal control report» as part of each annual Exchange Act report. For its definition see 15 U.S.C. § 7262. According to paragraph 15 U.S.C. § 7262(a), the report must affirm «the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting.» The report must also «contain an assessment, as of the end of the most recent fiscal year of the Company, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.» To do this, managers are generally adopting an internal control framework such as that described in COSO.

Both management and the external auditor are responsible for performing their SOX assessment in a top-down approach so that both the scope of the assessment and all evidence gathered are based *ex ante* on the whole range of risks that are relevant for the company. Such a top-down risk related approach offers the management wider discretion in its assessment. It is required to:

- Assess both the design and operating effectiveness of selected internal controls related to significant areas and the most relevant figures, in the context of material misstatement risks;
- Understand the flow of transactions, including IT aspects, in sufficient detail to identify points at which a misstatement could arise;
- Evaluate company-level (entity-level) controls, which correspond to the components of the COSO framework;
- Perform a fraud risk assessment;
- Evaluate controls designed to prevent or detect fraud, including management override of controls;
- Evaluate controls over the period-end of the financial reporting process;

25 SOX (Sarbanes Oxley Act) (2002)

26 Labaton and Oppel (2002: A1)

- Scale the assessment based on the size and complexity of the company;
- Rely on management's work based on factors such as competency, objectivity, and risk;
- Conclude on the adequacy of internal control over financial reporting.

The report's recommendations are that management and boards assume a leading role in ensuring that all risks facing a company are identified and assessed, and that a Risk Management and compliance system is in place to facilitate the proactive assessment, management, and mitigation of those risks. The Board of Directors (BoD) must make sure that it has fully appraised the risks faced by the company and that it can make an independent determination that management has implemented and maintained effective enterprise-wide integrated Risk Management policies and procedures, including internal controls and compliance.

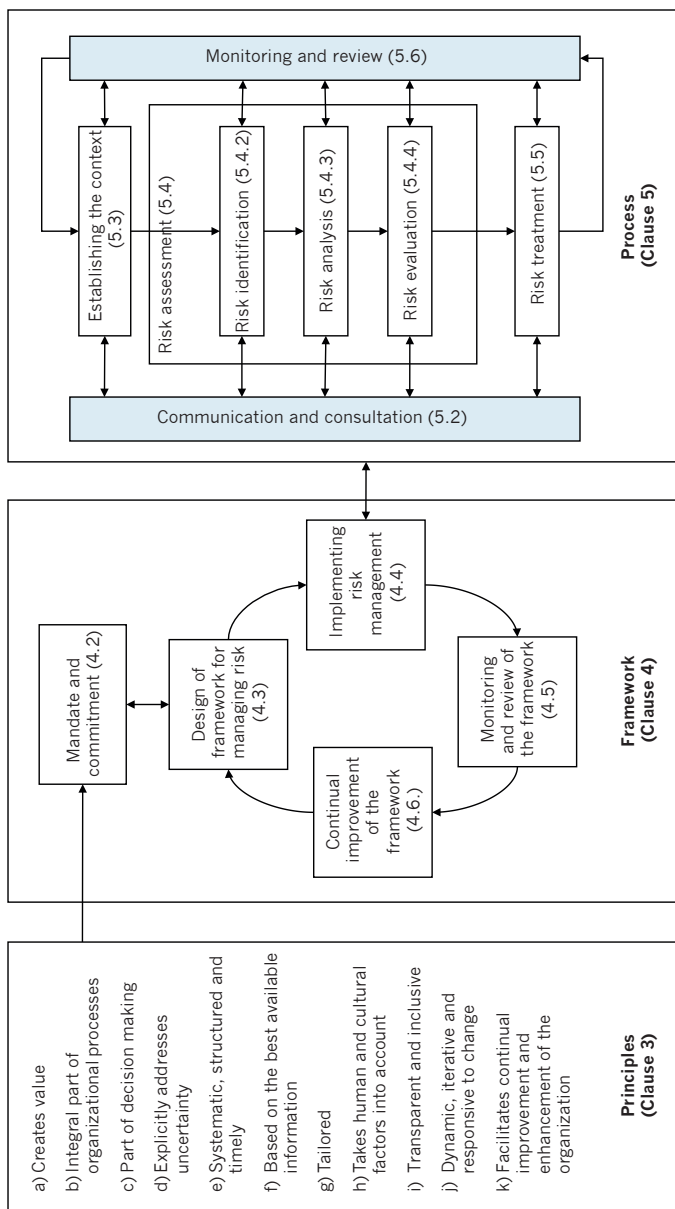
There was a general agreement from various stakeholders that the cost of SOX compliance was disproportionately higher for smaller companies. That has been largely resolved by some provisions in the recent amendments including the Dodd-Frank Act (2010) & JOBS Act (2012).

c) ISO 31000 & 31010 (Risk Management & Risk Assessment)

ISO 31000 was published as a standard in 2009 and contains generic guidelines for the design, implementation and maintenance of Risk Management processes throughout an organisation. This International Standard recommends that organisations develop, implement and continuously improve a framework the purpose of which is to integrate the process for managing risk into the organisation's overall governance, strategy and planning, management, reporting processes, policies, values and culture. The generic approach described in this International Standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context.

The relationship between the principles for managing risk, the framework in which it occurs and the Risk Management process described in this International Standard are shown in Figure 10.

Figure 10: Relationship Between Principles, Framework and Process



Source: ISO31000:2009

If the company standards are implemented and maintained pursuant to this International Standard, the management of risk enables an organisation for example to:

- Increase the likelihood of achieving objectives;
- Encourage proactive management;
- Be aware of the need to identify and treat risk throughout the organisation;
- Improve the identification of opportunities and threats;
- Comply with relevant legal and regulatory requirements and international norms;
- Improve mandatory and voluntary reporting;
- Improve governance;
- Improve stakeholder confidence and trust;
- Establish a reliable basis for decision making and planning;
- Improve controls;
- Effectively allocate and use resources for risk treatment;
- Improve operational effectiveness and efficiency;
- Enhance health and safety performance as well as environmental protection;
- Improve loss prevention and incident management;
- Minimise losses;
- Improve organisational learning;
- Improve organisational resilience

A supplement document to the ISO standard IEC/ISO 31010²⁷ was also subsequently published to help firms with various risk assessment techniques.

d) ISO 19600 (Compliance)

ISO 19600²⁸ standards on compliance management systems were first published in 2014. These standards define compliance to be an outcome of «an organisation meeting its obligations, and compliance is made sustainable by embedding it in the culture of the organisation and in the behaviour and atti-

²⁷ IEC/ISO 31010:2009 (Risk Assessment Techniques)

²⁸ ISO 19600: 2014 (Compliance Management Systems – Guidelines)

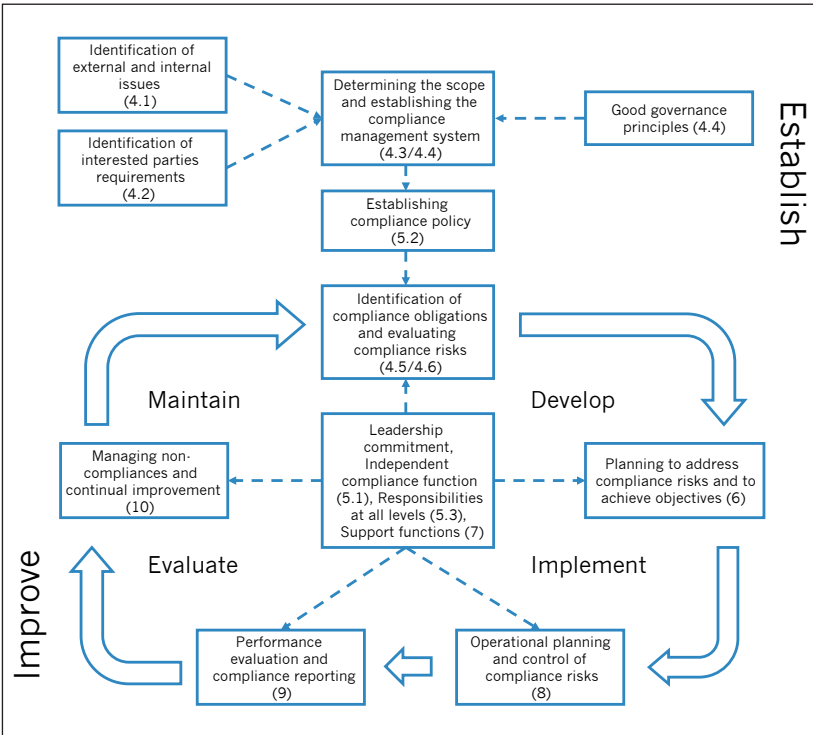
tude of people working for it. While maintaining its independence, it is preferable if compliance management is integrated with the organisation's financial, risk, quality, environmental and health and safety management processes and its operational requirements and procedures», thus clearly making the link between classical compliance issues of legal / regulatory compliance, ethics, integrity and regulations and Risk Management.

See below the compliance management system flowchart as recommended by ISO 19600, separating the Establish phase with the Improve (i.e. ongoing) phase.

The active involvement of and supervision by governing body and top management is an integral part of an effective compliance management system. This helps ensure that employees fully understand the organisation's policy and operational procedures and how these apply to their jobs, and that they carry out compliance obligations effectively. The standards amongst other, expect the organisational leadership to commit to:

- Establishing and upholding the core values of the organisation;
- Ensuring that the compliance policy and compliance objectives are established and are consistent with the values, objectives and strategic direction of the organisation;
- Warranting that policies, procedures and processes are developed and implemented to achieve compliance objectives;
- Making sure the integration of the compliance management system requirements into the organisation's business processes;
- Committing to alignment between operational targets and compliance obligations;
- Establishing and maintaining accountability mechanisms, including timely reporting on compliance matters, including noncompliance;
- Guaranteeing that the compliance management system achieves its intended outcome(s);
- Promoting continual improvement.

Figure 11: Flowchart of a Compliance Management System



Source: ISO 19600: 2014

II. Development of Risk Management

1. Overview of the Development Stages

The development of Risk Management can be divided into six stages:

- Stage 1 The beginning of new concepts and discussions in the field (1930s);
- Stage 2 The starting point of formal Risk Management, mainly dealing with credit risks (1970s);
- Stage 3 Focus on financial Risk Management, i.e. market Risk Management in addition to credit Risk Management (1980s);
- Stage 4 The idea of Operational Risk Management emerges, enlarging the field to operational risks (1990s);
- Stage 5 Enterprise Risk Management, i.e. taking a 360° view of Risk Management by integrating Risk Management across functions and divisions (2000 onwards).
- Stage 6 Heavily impacted by financial crisis of 2007-2008 and other catastrophic events (e.g. natural or nuclear disasters, climate change). Compliance had to newly enforce regulations and sustainability was becoming a crucial target for any kind of regulation.

Stage 1: New Concepts

The *starting point* of Risk Management can be isolated by security measures, including some loss prevention and a bundle of largely uncoordinated insurances.²⁹ According to Haller,³⁰ Frank Knight, John Maynard Keynes and John von Neumann wrote some important publications regarding risk and uncertainty in the 1920s. In the 1930s, the Glass-Steagall Act prohibited common ownership of banks, investment banks and insurance companies. In 1945,

²⁹ Haller (1999)

³⁰ Haller (1999)

Congress passed the McCarran-Ferguson Act, delegating the regulation of insurance to the various states.³¹

Stage 2: Credit Risk Management

Stage two occurred during the 1970s with the focus on insurance management, i.e. the co-ordination of insurance in its classic form of a risk transfer.³² Important landmarks for Risk Management in these years were the foundation of some associations with Risk Management as their target and scope, like the International Association for the Study of Insurance Economics or the «Risk Management Circle» of Sweden's Statsföretag. The American Society of Insurance Management was renamed Risk & Insurance Management Society (RIMS). Fortune magazine published the article «The Risk Management Revolution»³³ suggesting co-ordination of formerly unconnected Risk Management functions within an organisation and acceptance by the Board of Directors (BoD) of responsibility for preparing organisational policy and supervision of the function.

Stage 3: Financial Risk Management

The third stage was in the 1980s when the development of Risk Management diversified in two directions: One was *Risk Financing*, including concerted deductibles, captives and various mixed forms; the second was *Risk Control* in the sense of comprehensive risk engineering, partially in close co-ordination with insurance coverage. At the end of the 1980s, Risk Management experienced an expansion in the direction of risk communication, primarily as a consequence of a loss of trust after large-scale accidents in the concerned insurance sectors.³⁴ October 19, 1987 is still remembered as «Black Monday». On this day, the US stock market was severely hit, sending global shock waves and reminding all investors of inherent risk and volatility in the market.

31 Kloman (1999: 12)

32 Haller (1999)

33 Kloman (1999: 12)

34 Haller (1999)

Stage 4: Operational Risk Management

Stage four began in the 1990s. In certain industrial insurance markets, crises affected relationships between industrial insurers and big clients.³⁵ The term Chief Risk Officer (CRO) was for the first time used by James Lam at GE Capital describing the function of CRO to manage all aspects of risk.

Stage 5: Enterprise Risk Management

The 9/11 terrorist attack on the World Trade Centre, New York³⁶ has given a new dimension to the magnitude of volatility and risk. The New York Stock Exchange (NYSE) lost trillions of USD in a day. This had an enormous impact on the perception of Risk Management worldwide.³⁷ Today, companies embrace the concept of Enterprise Risk Management; this takes a 360° view of all risks facing the organisation, including internal and external ones, and looks to provide an integrated approach to manage risk across divisions and functions. This has furthered the establishment and development of concepts of Business Continuity Management where companies make sure that they survive even extreme events such as terrorist attacks, natural disasters, epidemics and major failures.

Stage 6: Compliance and Sustainability

The last few years have been shaped in large part by and as a result of the financial crisis of 2007-2008 which brought the entire world economy to the brink of disaster. The aftermath of that crisis is still perceptible for the markets in the form of local financial crises like the one in Greece, Spain and other economies of the world. Partially, the cause of the crisis was attributed to a lack of operational Risk Management and ethical behaviour. As a result, the regulators around the world have put forth a multitude of regulations, especially for financial institutions or for those companies having systemic impact on a national level within their jurisdictions and are thus considered «Too Big To Fail».

35 Haller (1999)

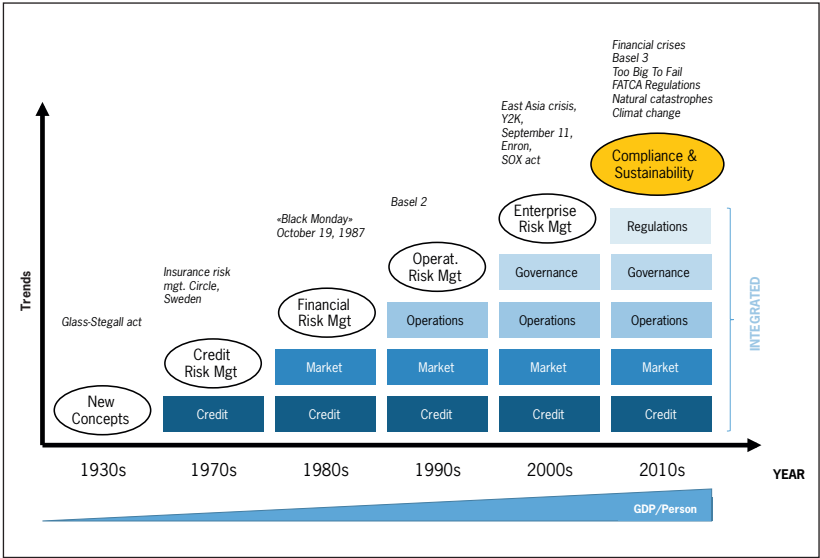
36 Ernst & Young (2002)

37 Ernst & Young (2002)

In addition, the world has also witnessed many natural catastrophes (chronic famines in Africa; tsunami in Japan, floods in several geographical regions) and man-made disasters (e.g. accident of Fukushima Nuclear plant in Japan) which have put the future of the planet at stake and emphasised the importance of sustainable management and corporate citizenship. Rather than being passive observers, organisations are being expected (both voluntarily and by law in certain aspects) to play a pro-active role in combating such serious events or developments.

Figure 12 provides a graphic view of these developments. The interesting thing to observe in this figure is that the growing affluence of the world (represented by growing GDP) has also put more focus on Risk Management. It also demonstrates that the current interest in Risk Management is not temporary and is only going to increase further in the coming years.

Figure 12: Evolution of Risk Management



Source: Adapted from various sources

- Principle 4.10: The board should ensure that there are processes in place enabling complete, timely, relevant, accurate and accessible risk disclosure to stakeholders.

f) The Basel Committee Reports

The Basel Committee on Banking Supervision (BCBS) was established as the committee on Banking Regulations and Supervisory Practices by the central bank governors of the group of ten countries at the end of 1974, in the aftermath of a serious monetary crisis providing a forum for regular co-operation between its member countries.⁵⁷ The committee has focused mainly on capital adequacy and risk measurement, on and off balance sheet. In 1988, the Basel capital accord was implemented which, after amendment in 1995, included that the senior management has to be responsible in managing credit risks from exposures in derivative products and other add-on factors.⁵⁸ Market risk was added to that accord in 1996. Such risks may occur from the bank's open positions in foreign exchange trade, debt securities, equities, commodities, and options. In 1998, the committee also covered operations risk on its agenda⁵⁹, and the accord is widely known as *Basel II Capital Accord*. Because of this accord awareness of operational risk as a separate risk category has increased. Various aspects relating to defining operational risk such as measurement, monitoring, control, policies and procedures have been discussed and established. In a broader sense, operational risks are accepted as those risks which are not covered under market and credit risk, like legal risks.

Basel III⁶⁰ is a comprehensive set of reform measures developed by the Basel Committee on Banking Supervision, to strengthen the regulation, supervision and Risk Management (special focus on operational risks) of the banking sector. These measures aim to:

- Improve the banking sector's ability to absorb shocks arising from financial and economic stress, whatever the cause;

57 Basel Committee (Risk Management Group of the Basel Committee on Banking Supervision) (2003)

58 Basel Committee (Risk Management Group of the Basel Committee on Banking Supervision) (2003)

59 Basel Report (1998)

60 www.bis.org

- Improve Risk Management and governance;
- Strengthen banks' transparency and disclosures.

It was agreed by the members of the Basel Committee on Banking Supervision in 2010–11 and was scheduled to be introduced from 2013 until 2015; however, changes from 1 April 2013 postponed the implementation deadline to 31 March 2018 and later again to 31 March 2019.

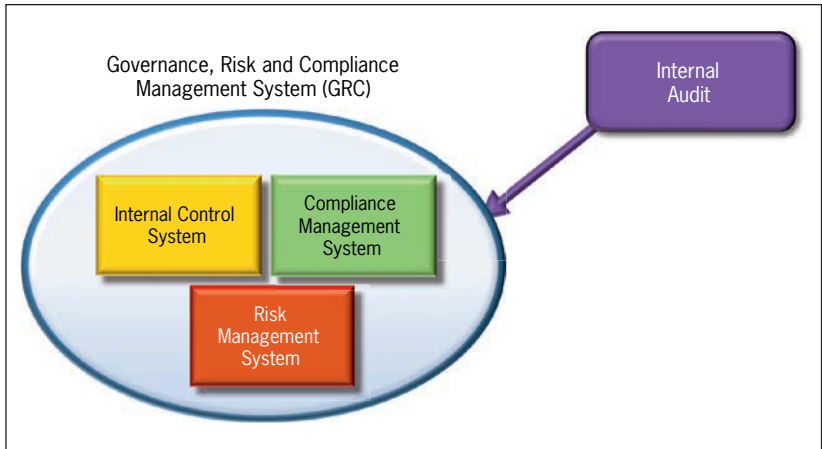
3. Risk Compliance

Risk Management and Compliance Management are closely linked and both are part of the Corporate Governance. In accordance with Art. 716a CO, the Board of Directors of a Swiss corporation is ultimately responsible for the overall management of the company. In this regard, the board must ensure that the company's strategic objectives are in reasonable proportion to the resources available. Thus the corporate strategy should remain within the overall scope of the company, which still leaves room for modifying the strategy to be more owner-related. Thereby it is essential that the board (e.g. through an audit or risk committee) analyses all risks resulting from the implementation of the corporate strategy and mitigates them wherever possible. In this context, the risk potential constituted by all internal and external rules and regulations that have to be adhered to and complied with is considerable. That major risk area is called Compliance. The basis of compliance is therefore a Risk Management system that allowing the key risk areas to be identified.

The Compliance Management System (CMS) of a company complements the existing Risk Management system on which the Internal Control System (ICS) is based. It may be of advantage to structure the CMS of an organisation along the recommendations by the ISO 19600 guidelines. This should ensure the adherence to all applicable statutory provisions, international standards like those of the Financial Action Task Force (FATF) on money laundering and internal policies and guidelines (e.g. a Code of Ethics) on all levels throughout the company. This ultimately leads to a responsible and transparent corporate management that is part of the corporate governance.

In addition to the three systems mentioned above, i.e. Risk Management or Compliance Management System resp. Internal Control System, the BoD may introduce the control function of an Internal Audit, with the mandate and goal to conduct independent reviews in all areas of the company. Graphically, the interaction of all functions in a company is illustrated below:

Figure 14: Governance, Risk and Compliance Management System (GRC)



Source: Own illustration

a) Establishing of the Compliance Function at the Executive Level

Compliance is an undelegable and inalienable responsibility of the top strategic level of a firm. Even if the BoD entrusts a Compliance Committee or a Compliance Officer with the mandate to warrant adherence to all applicable regulations, the board itself remains ultimately responsible for the effectiveness of the compliance management system. Therefore, the board should deliberate carefully what executive levels are most appropriate to keep the compliance function effective.

According to par. 18 of the recommendations of the Financial Action Task Force (FATF Recommendations) of 2012⁶¹, all financial institutions are expected to implement the FATF standards and provide for appropriate measures. This is substantiated by the third Interpretive Note as follows: «Compliance management arrangements should include the appointment of a compliance officer at the management level.» Article 84 of the EU Directive 2013/0025 (so-called 4. Money Laundering Directive) includes a similar stipulation: «The policies and procedures referred to shall at least include: the development of internal policies, procedures and controls, including customer due diligence, reporting, record keeping, internal control, compliance management (including, when appropriate to the size and nature of the business, the appointment of a compliance officer at management level) and employee screening.» Both quoted directives request that there be a compliance officer at the executive company level. Would that imply that a compliance officer should be a member of the top management / executive board? This will be a wrong conclusion to derive. On the contrary, the opposite may be appropriate, as the Compliance Officer has a clear guarantor position by law (Garantenstellung). In this role Compliance Officer is expected to prevent all business / transactions that could lead to breach or infringement. As a member of the Executive Board, he may be inclined to accept any business deals for the sake of high profits, even if that would mean higher risks. The contradiction of roles inevitably leads to an irresolvable conflict of interest.

Ideally, the board appoints a Chief Compliance Officer (CCO) who, though on the level of the Executive Board, is not himself member of it and therefore independent. In such a set-up, the CCO may report to the CEO on a regular basis, but may also report directly to the Chairman if appropriate. Conversely, the chairman of the board can use the CCO in addition to the Internal Audit to fulfil its overall compliance requirements. The Board of Directors must ensure that it is periodically informed about the activities of the CCO or the compliance department. The board should intervene if the compliance activities and trainings are deemed insufficient.

61 FATF (2012)

b) Guidelines for Compliance Management System

In December 2014, the ISO standard ISO 19600 was published. It is the first international standard for compliance management systems (CMS). The aim of ISO 19600 is to provide internationally supported guidelines for the design, implementation, operation and continuous improvement of effective CMS by public and private organisations.

Organisations of all types, i.e. private and public companies, governmental agencies and NGOs are expected to follow the recommendations. Deviations from the word of the standard is possible, but solely on condition that the different measures are still living up to the spirit of the standard (comply or explain). Large companies, especially if operating in various countries, and government agencies as well as non-governmental organisations with activities in sensitive regions or industries should introduce a Compliance Management System, be it according to ISO 19600 or similar⁶². Such recommendation is indirectly supported by various judgments. On 10.12.2013, for example, the Munich District Court condemned a former CFO of Siemens AG and solicited damages of approx. EUR 15 million for his violation of obligations, i.e. failure to establish an effective compliance system to avoid bribery and corruption. In January 2015, the British Financial Conduct Authority (FCA) has ruled that the CEO and the Compliance Officer of Martin Brokers (UK) Limited had to pay fines and banned from profession. This because they allegedly contributed to a culture which permitted manipulation of the LIBOR and assumed that such manipulation would not be detected soon enough. The two directors did not seem to have made any efforts to prevent this culture of malpractice.

c) Elements of a Compliance Management System (CMS)

The elements of a compliance management system can be divided into «soft factors» (good leadership, management of values, culture of integrity and law-abidance) and «hard factors» (organisation and processes). According to ISO 19600, the key elements of a CMS are:

⁶² Voluntary code; no regulatory obligation

- Good leadership; the organisation's values and compliance culture;
- Implementation of the principles of good governance;
- A compliance strategy that is approved by the top management (Compliance Policy);
- The organisation of compliance roles, responsibilities and competencies;
- The processes;
- Assessment of effectiveness;
- The improvement of the CMS.

To prevent illegal behaviour or violations of the Business Conduct Guidelines (e.g. Code Of Ethics) effectively, the Board of Directors and the Executive Board of a company must be able to rely upon the fact that information of impending misconduct, already occurred violations or of other adverse conditions is being reported immediately to the appropriate authorities. If possible, such information should disclose the person reporting the violation. But if that is not possible for any reason, an internal or external whistleblowing office / hotline should be established to facilitate anonymous reporting of such incidents. This aids an effective CMS⁶³.

Detected or suspected violation should be reported without delay, usually to the direct line manager. If this manager is very likely not to act upon receipt of the information, or if the employee is bound to face reprisals, or in case the violation reported relates to line manager himself, the reporting should be addressed to the internal whistleblowing office / hotline of the company. In case the reported situation does not improve after the notification to the whistleblowing office, or if a reporting to the internal whistleblowing office appears futile from the outset, e.g. because the internal whistleblowing officer is being inflicted by the reporting, the reporting should be made to the external whistleblowing authority (hotline, website or office).

Employees that have to file a notification to a whistleblowing office should have the right to remain anonymous. This means in practice that the whistleblowing office knows neither the name nor the function of the reporting person. In addition, the content of the message is summarised and anonymised

63 For complete reglement of whistleblowing, refer to Müller, Lipp, Plüss (2014: 1161 ff.)

so that no conclusions about the whistleblower are possible. In essence, a whistleblowing system should ensure that:

- Potential violations are reported;
- Employees do not feel hindered to speak up for fear of retaliation (e.g. in sexual harassment cases where someone does not dare to report it to his / her boss as that boss was the perpetrator);
- A hotline serves as an effective tool where employees cannot report issues to their direct line manager (or ombudsperson or HR);
- Whistleblowing policies offer the opportunity to report anonymously, to make it as easy as possible for the employees to speak up.

The figure below shows an overview of the various systems of an enterprise. Managing their inter-linkages and overlaps presents a challenge for the strategic management.

Figure 15: Relationship Between Various Risk Management Processes



Source: Own illustration

VI. Managing Fraud and Corruption Risks



Peter Jonker

Peter Jonker is a director at the 4N6 Factory, a Zurich based consulting boutique, supporting companies with both forensic investigations and development and implementation of corporate compliance and integrity programs. Before joining the 4N6 Factory in 2012, Peter worked as an advisor for the Dutch and Swiss branch of a Big Four Consulting firm for 14 years. Currently he is a member of the UN Global Compact Working Group on

Anti-Corruption (Principle 10) in New York and serves as a lecturer in «Ethics and Leadership» at the Executive MBA-programme of the University of Zürich. Peter holds a Bachelor degree in Economics and Business Administration, studied Policy Sciences and Organisation Studies (Drs.) at the Tilburg University in The Netherlands and absolved a post-doc at the ISAM institute of the Erasmus University in Rotterdam.

1. Problem Overview

According to the Association of Certified Fraud Examiners (ACFE), a company loses approximately 5 % of its annual revenue on occupational fraud and misconduct¹²⁶. Another US study shows that on average a company receives 9.27 hotline calls per 1,000 employees per year¹²⁷.

Many CEOs in European companies will counter that these results are not representative for their company. In addition, where it is common for US companies to have a hotline to report (potential) violations, ethics hotlines remain a sensitive topic in the larger part of Europe. Still, the question

¹²⁶ ACFE (Association of Certified Fraud Examiners) (2014)

¹²⁷ The Network In. (2013)

remains if US companies are so much more corrupt, or if in European companies non-compliance is detected in other ways.

In this light a study by the HTW in Chur¹²⁸ offers an insight in the exposures of Swiss SMEs in doing international business. Of the 510 participating companies, over 40 % indicated informal payments or gifts were expected from clients and business partners. Over half of the companies exposed to these requests actually paid, on average amounting to 4.9% of their annual revenues in those countries.

Naturally, a business gift or an invitation to a business dinner does not necessarily constitute a bribe. Nor is a voluntary contribution to a political party automatically a form of corruption. So, when does this gift turn into a bribe? Or when is entertainment 'lavish'? In identifying a company's exposure to fraud and corruption risks, we need to consider a few complicating factors.

a) Clarity of Norms

First of all, the norms are not always clear. Not only because of differences in local business customs or local laws and regulations but also because of the changes over time; for example, a facilitation payment used to be tax deductible as a normal business expense in Europe just twenty years ago. The trend clearly goes towards tighter regulation, but when employees do not know what the standards and rules are, they cannot be expected to uphold them.

At the same time, in Europe, most companies prefer a principle based approach instead of a rule based approach. Unlike US Codes of Conduct, European companies often communicate their values and principles at a very high level, leaving room for – and the challenge of – interpretation to their employees.

Appendix 16 (Elements of a Code of Conduct) provides an overview of what a typical Code of Conduct entails.

b) Risk of Being Caught

A second development is the increase of enforcement initiatives to counter fraud and corruption in recent years. Where in the EU the enforcement

128 Hauser (2012)

trend focused more on Anti-Competition (cartels etc.), the US have been using their Foreign Corrupt Practices Act (FCPA) to fine companies that have bribed (government) officials abroad. Meanwhile, also other countries (e.g. UK, Brazil, Canada) have defined laws with a so called «extra territorial» reach and start enforcement initiatives.

Many CEOs and board members in Europe are not aware (or simply ignore) these rules also apply to their company. If a Swiss company is bribing an Asian government official (or hires an agent to do this on their behalf) and (allegedly) pays in US dollars, this already is enough reason for the US authorities to investigate a (potential) violation of the FCPA; irrespective if the company has a listing or a subsidiary in the US. In Brazil, under the new anti-corruption law (for violations within Brazil AND abroad) the corporate fines can amount to 20 % of the company's annual revenue.

Also in China, the new Government started with a Bribery and Corruption crackdown, for instance in the Pharma sector. Apart from corporate fines, in China far more executives and officials are being sent to prison. All in all, temperature is rising and the risk of being caught and fined grows significantly.

c) Difficulty to Discuss

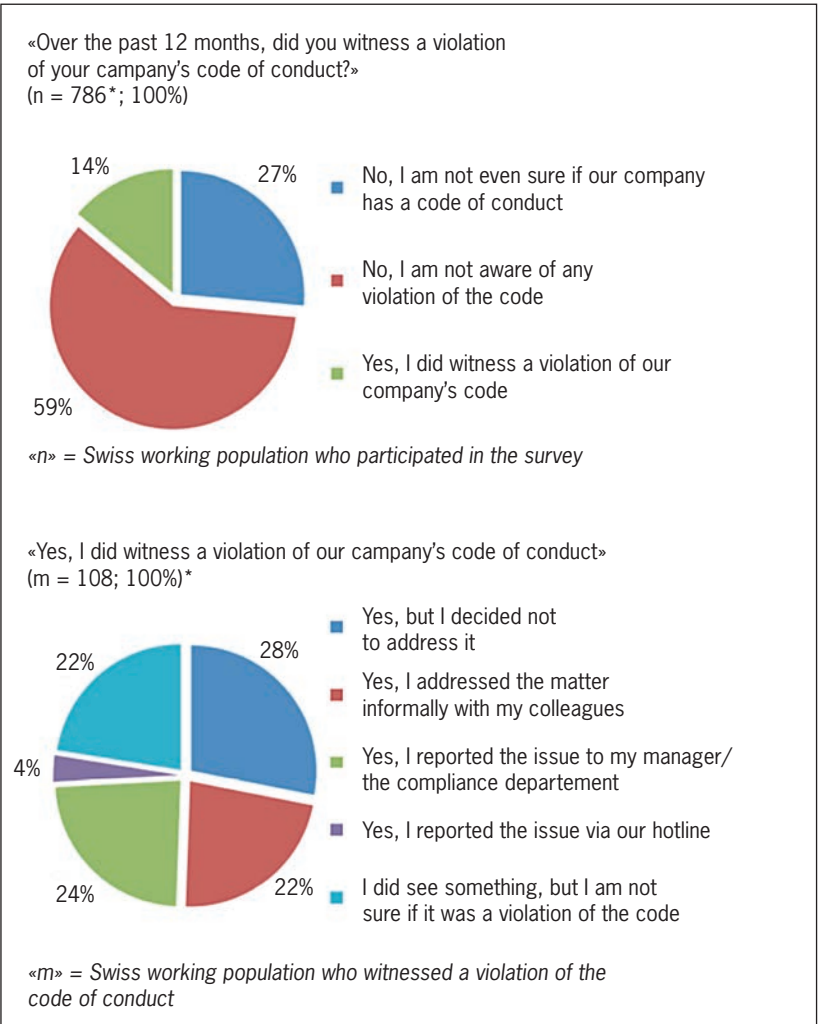
A third complicating factor is the fact that it is difficult to address (potential) unethical business practices. With the excuse of «being in a country with a different business culture», «severe business pressure» or «everyone else is doing it», CEOs and board members will be tempted to look away.

The big elephant in the boardroom therefore is the question «are we prepared to walk away from business»? Without a clear tone from the top, local managers will interpret their new sales targets as «go with God, come back with money» – also since their performance will be measured and rewarded on financial KPIs.

For employees, it is also difficult to address potential violations. A recent study¹²⁹ by the 4N6 Factory and market researcher GfK under the Swiss working population showed that 14 % of the Swiss employees did witness a violation of their company's code in the last year.

129 Webpoll under Swiss working population (n=1200), 4N6 Factory and GfK, 2014

Figure 34: Occurrence of Code of Conduct Violations



Source: 4N6 Factory and GfK, 2014

Only 28 % of the employees who witnessed a violation reported the issue to their management, the compliance department or the company hotline. In

Switzerland, 72% of the potential violations are not reported. Other international studies show the main reason people do not report potential violations is the fear for retaliation from supervisors or co-workers¹³⁰.

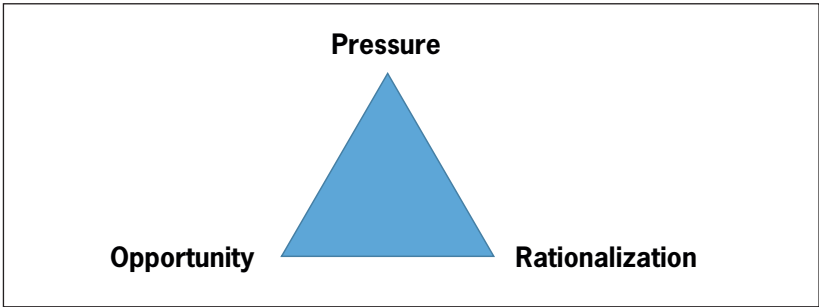
d) Intentional Act

Unlike many other operational risks discussed in this book, fraud and corruption risks are unique in their character as they are <intentional>. A fraudster seeks to harm the company on purpose and a bribe is paid with the intention to induce someone to act in favour of the bribe payer. This means that – despite controls that are put in place to prevent fraud and corruption – the fraudster is actively looking for ways to circumvent controls without being detected.

2. Who are Involved?

According to Donald Cressey’s <Fraud Triangle>¹³¹ the risk of fraud or corruption depends on three elements; Pressure, Opportunity and Rationalisation.

Figure 35: The Fraud Triangle



Source: www.acfe.com/fraud-triangle.aspx

«Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to

130 Ethics Resource Center (2012)

131 www.acfe.com/fraud-triangle.aspx

*apply to their own conduct in that situation verbalisations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property.»*¹³²

In principle, everyone that is under enough pressure (for instance sales targets), sees an opportunity to commit fraud (‘no one will find out’) and finds a rationalisation for his behaviour (‘others are doing it as well’) could be tempted.

An analysis of historical data gives more insight on the perpetrator’s profile¹³³:

- Usually Male (66.8 %);
- Between the age of 30 and 50 (66.2 %);
- No prior conviction (86.6 %);
- Working for the company for 6 years or longer (52.5 %);
- Often working in Accounting (17.4 %), Operations (15.3 %), Sales (12.5 %) or Executive or Upper Management (11.8 %).

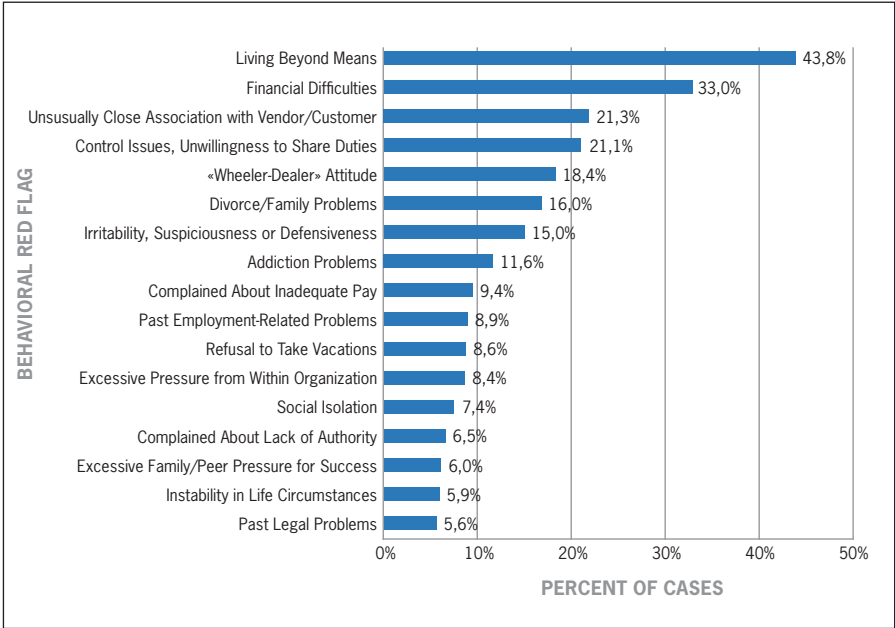
a) Red Flags

There are some behavioural warning signs that a perpetrator in a fraud case might demonstrate. In many cases of fraud and occupational misconduct, the perpetrator was living beyond his means (43.8 %) or was having financial difficulties (33 %). (see Figure 36)

¹³² Cressey (1973)

¹³³ ACFE (Association of Certified Fraud Examiners) (2014)

Figure 36: Behavioral Red Flags Displayed by Perpetrators



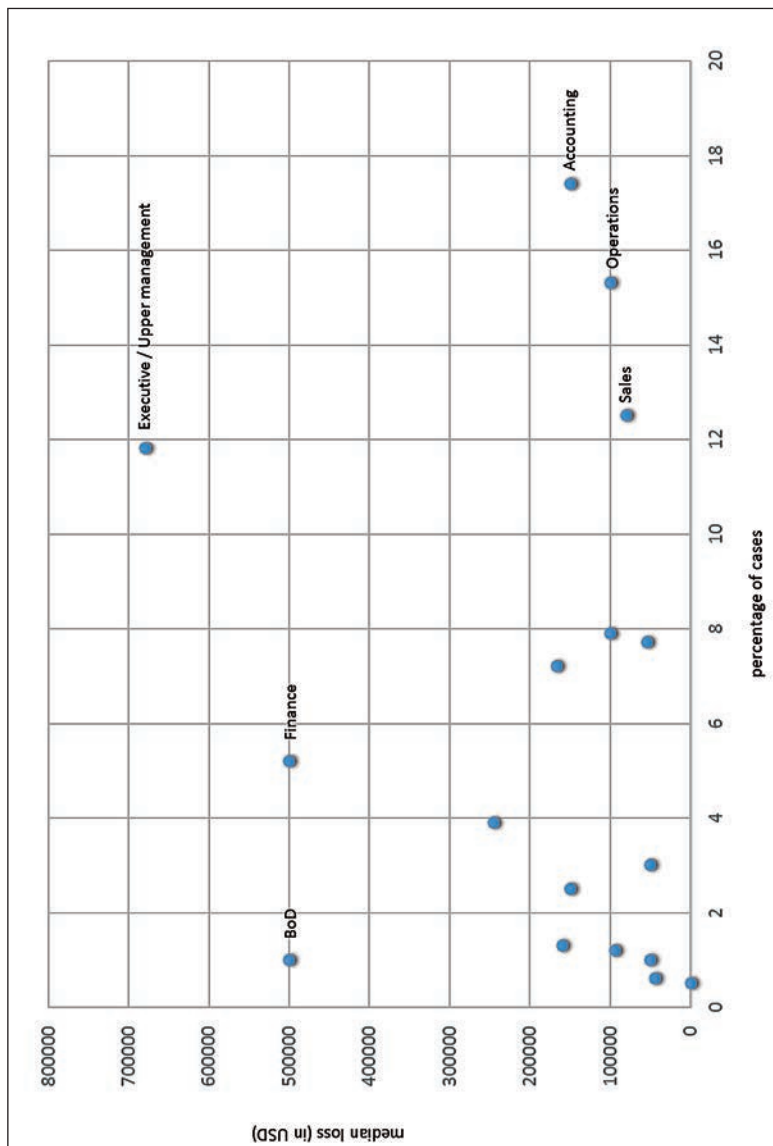
Source: Association of Certified Fraud Examiners, Report to the Nations on Occupational Fraud and Abuse, 2014

b) Departments Involved in Fraud Cases

The graph below shows in which departments perpetrators were working and what the median loss was in those cases. The losses are greater when senior management, the Board of Directors or finance are involved. Quite often, perpetrators are working in one of the following departments: Accounting (17,4 % of the cases), Operations (15,3 %) and Sales (12,5 %).

Relevant for board members is the fact that the highest losses are suffered right under their nose: in 11,8 % of the cases, when Executive/Upper management are involved, the median loss is USD 680,000 USD per case.

Figure 37: Departments Most Likely Involved in Non-Compliance Cases



Source: Adapted from ACFE (Report to the Nations on Occupational Fraud and Abuse, 2014) by 4N6 Factory

3. Common Forms of Corruption

Fraud and corruption can take many shapes and forms. The Association of Certified Fraud Examiners distinguishes between three different categories: Corruption, Asset Misappropriation and Financial Statement Fraud (see Figure 38).

In this paragraph we will zoom in on the first category 'Corruption' to identify a few of the more common schemes in (international) business.

a) Gifts and Entertainment

Gifts and entertainment are a normal part of business in many countries. And usually not illegal either. But to distinguish between what is appropriate and what is 'lavish' is sometimes difficult. It not only depends on local business customs and laws, but also on the timing; is it appropriate to invite a potential client for a dinner in the middle of a tender phase? This could be perceived as bribery, when one wants to influence the decision making (see facilitation payments and bribes).

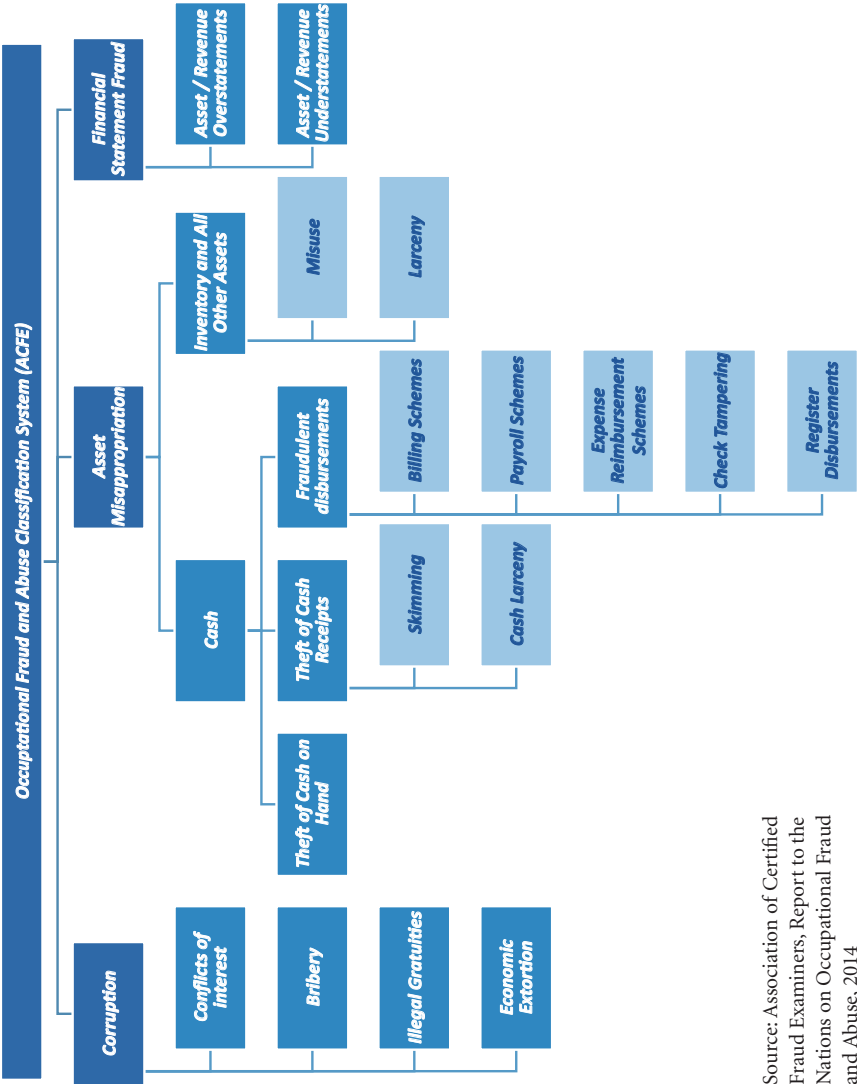
b) Facilitation Payments and Bribes

A facilitation payment (also facilitating or 'grease' payment) is a small payment to foreign officials to speed up administrative processes (e.g. customs clearing, police official giving safe passage). Some laws and conventions distinguish a facilitation payment from a bribe, others claim facilitation payments are bribes as well. Bribery is often defined as 'the offering, giving, receiving, or soliciting of any item of value to influence the actions of an official or other person in charge of a public or legal duty'.

c) Kick-backs and Overbilling Schemes

A kickback is a form of negotiated bribery in which a commission is paid to the bribe-taker as a 'quid pro quo' for services rendered; for instance when the head of a procurement department receives a commission of 5 % on the total order volume from supplier A, when selecting this provider. The money is paid into the head of the procurement's personal account (so not a discount of which the company benefits). Usually the supplier will send inflated invoices for his products and services afterwards (overbilling scheme), which procurement will then approve.

Figure 38: The Fraud Tree



Source: Association of Certified Fraud Examiners, Report to the Nations on Occupational Fraud and Abuse, 2014

d) Bid-rigging and Price Fixing

This situation occurs when vendors work together in bidding situations and agree on who will offer for the lowest price, in order to win the project. Another vendor will bring the lowest bid at a next tender opportunity. This situation can arise especially in an oligopolistic market or when suppliers have to make huge investments (time and money) to write a tender (e.g. in infrastructure projects in oil and gas, rail, roads, tunnel building or large property development).

e) Use of Agents

For many companies aiming to expand into other countries, the use of sales agents or distributors is the first step; they know the market, local language and business context and have a network. Often, the agents work on a commission basis; they get a percentage of the total sales volume, when the deal is made. For the company an attractive model as they have to pay out only when they win work. The agent however, will do everything to close the deal. If that means bribing a government official to win the job, this is merely a 'business expense' to him. The commission is simply split between the agent and the new-won client. Although still common practice in many countries, there are some legal changes which make this model less attractive; a company that asks a third person (the agent) to act on their behalf, is still accountable for these actions as if it was their own employee.

f) Political Support and Charitable Contributions

In many countries donations to political parties and charitable contributions are a normal business practice, tax deductible and sometimes even seen as 'good citizenship'. However, this financial support can easily become a form of bribery. For instance, when a company will be granted the permission to build a factory, *under the condition* they also make a 'voluntary' contribution to a political party or charitable fund to send promising local students abroad to get a good education. Most likely the political party and children of the decision makers will benefit from these contributions.

The RESIST Methodology in Appendix 13 provides further scenarios for corruption. In addition, detailed samples of specific rating criteria for cor-

ruption related scenarios can be found in International Chamber of Commerce, Transparency International, United Nations Global Compact, World Economic Forum publication.¹³⁴

4. Managing the Risk of Fraud and Corruption

When determining the fines in large corruption or cartel cases, governments explain their rationale and as a consequence define what a good compliance program should look like. The US government was among the first when defining the Federal Sentencing Guidelines, requiring companies to have an «Effective Compliance and Ethics Program» and explain what this entails. The 2011 UK Bribery Act defines six principles and offers guidance in the form of concrete cases.

In September 2014, a working group of Swiss Holdings and Economiesuisse presented guidelines for compliance management¹³⁵. In addition, the International Standards Organisation (ISO) has been developing a new standard for compliance Management: the ISO 19600 standard.

There are quite a few overlaps between the standards and guidance documents. The graph below summarises the most important elements¹³⁶.

134 International Chamber of Commerce, Transparency International, United Nations Global Compact, World Economic Forum 2011

135 Jaisli (2014)

136 4N6 Factory (2014)

Figure 39: Elements of Fraud Risk Management Framework



Source: 4N6 Factory (2014)

This starts with a proper assessment of bribery and corruption risks (1) the company is exposed to (and the controls to mitigate them). Clarity on roles and responsibilities (2) supported by written policies and guidelines (3) are implemented using training, communication and other awareness initiatives (4 and 7). In addition, a process to detect (5) and respond (6) to fraud and other forms of non-compliance should be in place. A final element of a good compliance program, consists of due diligence on business partners and prospective employees (8).

a) Effective Compliance Programs

Having a Fraud Risk Management or Compliance Framework is one thing, making sure that it is effective and actually lived, is quite another one. This is why there is a clear trend to focus on softer elements, starting with the tone

at the top» (and the tone at the middle). As a first step, many companies publish a «Code of Conduct»¹³⁷, where the CEO or Chairman of the Board write a foreword or introduction stressing the importance of the company's values and principles. But, a code could easily become a paper tiger, when management does not lead by example and employees do not feel comfortable to seek guidance when they have ethical concerns or report a violation when they see one.

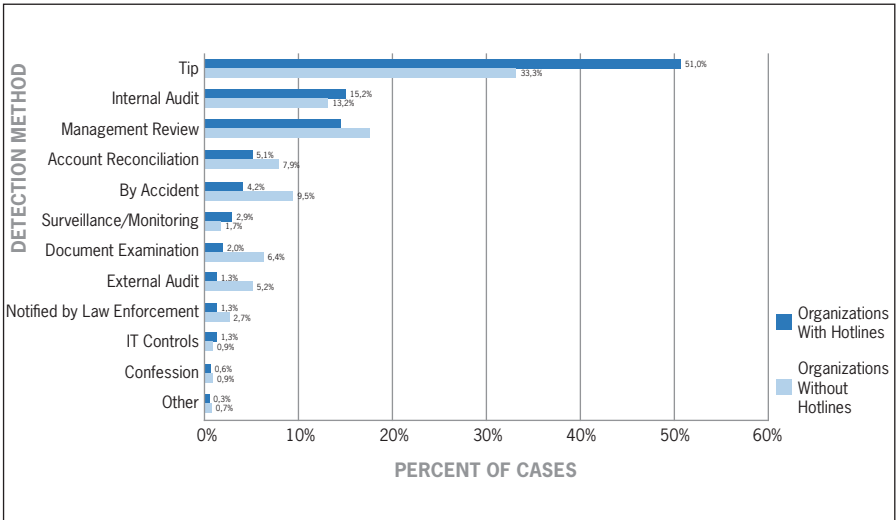
Hotlines

Although in Swiss companies a hotline is not a popular instrument, international studies show that it is one of the most effective ways to detect misconduct¹³⁸. The graph below shows most cases of misconduct have been detected by a tip. This includes hotline calls but also other tips via (anonymous) letters or tips from clients and suppliers. In companies with a hotline, over half of all cases have been detected by tips.

137 See Appendix 16 (Elements of a Code of Conduct)

138 ACFE (Association of Certified Fraud Examiners) (2014)

Figure 40: Impact of Hotlines



Source: ACFE (2014)

Measuring effectiveness

Measuring if a compliance programme has been effective, also requires changes in the compliance officer's KPI set; knowing the participation and completion rates of the e-training is no guarantee if the corporate code of conduct is actually lived.

The focus of measuring the effectiveness of compliance programs shifts from 'input' (e.g. budget and FTE) and 'output' (e.g. training hours, completion rate of e-training) towards 'outcome' (guidance requests) and 'impact' (e.g. termination of contracts with non-compliant suppliers).

A next challenge will be to address these new KPIs in the context of performance measurement and incentives, which in turn will lead to a new discussion on target setting.

For the Board of Directors and executive management the fore mentioned key question to answer will be 'Are we prepared to walk away from business?' Without a clear tone and actions from the top, the organisation will meet its targets ('what') at the expense of the 'how'.

VII. Risk Management of Major Projects



Dr. Stephan Werner Döhler

Prior to his current position as the CEO of Swiss nuclear power plants Leibstadt and Beznau and the Head of the Nuclear Division at AXPO Ltd., Stephan Werner Döhler served in various management positions at ABB and Alstom. Today he is a member of the management board of Axpo Power Ltd. and board director or chairman at several companies in Switzerland and Germany. He holds a Master of Technical Sciences from Zittau Tech-

nical University, a PhD from Moscow Power Engineering University (MEI) and an MBA from Business School Lausanne. He lectures Thermodynamics at the University of Applied Sciences North West Switzerland and Risk Management at the University of St. Gallen.

1. Why Risk Management of Projects at Board Level?

Every project has its specific risks. While project risk management is obligatory in most companies with well-developed managing processes, it is usually considered a part of the company's operative business and thus not falling necessarily into the competence of the board. Some projects, however, may represent a risk for the entire company – either because of the considerable amount of investment involved or due to the significant exposure of the company's reputation. For this category of projects risk management needs to be organised at the company level, and the Board of Directors should be in charge and kept informed by means of regular status reports.

Unfortunately, this is not always the case. For instance, in large-scale projects carried out in the public sector, governmental or regional organisations

tend to underestimate the importance of professional project management and risk control.

There are many examples demonstrating quite clearly how projects – or just one single project for that matter, – can cause the exposure of the entire company to a major risk or even its fall. Enron projects including the multi-billion Dabhol Project in India¹³⁹ and Windreich bankruptcy due to offshore wind farms¹⁴⁰ illustrate how severe consequences of a failure of a large project or insufficient project risk management may be.

Political or societal processes bringing about dramatic changes in the market environment frequently trigger difficulties in project execution. Companies and civil structures involved often find themselves utterly unprepared for the changes and experience major difficulties while coping with the new conditions and/or limitations. A classical example is the paradigm shift happening on the European (and Swiss) power generation market.

Projects have always been a complex business, and never a fully controllable one. The success factors are multiple, the involvement of competent people and a good organisation being crucial. Yet even in the best-organised company there is no guarantee against delays, budget overspending or failures in general, when it comes to projects. Project-related risks can be limited, although not eliminated, by following a set of rules and processes, which is of paramount importance for company boards. Whenever a company or organisation is faced with a major project – i.e. one involving a substantial amount of investment and/or resources, – it is important that the company's Board of Directors follow a number of routines and procedures to assess and mitigate the risks. The sections that follow provide an overview of some important basics, processes and documents that constitute a prerequisite for project risk management and need to be implemented at the board level.

139 The rise and fall of Enron, reported from the San Jose State University, Department of economics, Thayer Watkins, PART: Foreign Projects

140 «Windreich: winded», the bankruptcy of the German leader in the field of offshore wind farms, reported from the journal «HANDELSBLATT», 09.09.2013, 18:36

2. Risk Management Guidelines

Risk Management Guidelines is a document issued by the Board of Directors in which key rules, conditions and limitations relevant to risk management are defined. It provides a common basis for understanding risk management processes and terminology in a given company. It also contains a description of crucial processes, organisational structure and responsibilities within the company. Risk Management Guidelines should clearly identify all relevant laws and regulations and ensure their implementation at all levels of risk management.

Being the master document for any further risk management documentation and process descriptions used by the company,¹⁴¹ Risk Management Guidelines focus on the overall boundary conditions and long-term data. The examples below highlight some elements of Risk Management Guidelines corresponding to managing specific project-related risks:

ISO 31'000 for Major Projects

Risk management terminology as well as the description of all processes and project-related risks can be found in ISO 31'000.¹⁴² The entire risk management process should be organised in accordance with the country legislation in force taking into account all relevant special regulations.

COSO-ERM Framework for Major Projects

COSO Enterprise Risk Management Framework published in 2004¹⁴³ is another important international instrument. It links company goals to its organisational structure and the adopted risk management system. Both models (ISO 31'000 and COSO) provide for a reliable and functional basis for risk management at the company level.

Compliance

The term «compliance» means respecting all international and national laws, rules and regulations as well as the company's internal standards and rules.

141 Department of Treasury and Finance (2004)

142 ISO 31'000 (2009)

143 COSO (The Committee of Sponsoring Organisations of the Treadway Commission) (2003)

Compliance is of outmost importance for the purposes of project-related risk management, especially given the globalised nature of modern project business exposing companies to a multitude of laws, rules and regulations that range from tax regulations to labour migration issues (e.g. obtaining work permits for employees working abroad or for foreign nationals coming to the company headquarters). Furthermore, there is evidence of alarmingly growing exposure of international projects to bribing and corruption practices.¹⁴⁴ In order to adequately handle the totality of risks in line with the current legislation, companies need to address all of the above in their project-related risk management processes and compliance codes. In addition to their practical value, risk management processes and compliance codes are powerful communication tools standing for the company's commitment to law abidance, ethics and integrity.

Investment Process

Risk management in project business begins at the investment stage. For many companies, project-related investments account for a substantial, if not dominant part of their total investment budget. Hence the importance of having a structured investment process and implementing a long-term planning and strategy including proper risk management processes. In addition to participating in the long-term investment planning, risk-managers need to be involved in the investment process as early as at the level of a single major project.

Categories of Risks in Major Projects

In order to account for all possible internal and external risks in major projects, a number of risk categories are assessed. Most commonly, following categories of risks are taken into account:¹⁴⁵

- *Market risks:* These are risks caused by changes in fundamental market indicators, such as prices, exchange rates and/or interest rates. Market risks are extremely sensitive to changes in the legal and regulatory framework;

¹⁴⁴ Sanyal (2005)

¹⁴⁵ Cf. PWC (2008); Department of Treasury and Finance (2004)

- *Counterpart-related risks*: Risks caused by non-fulfilment of contractual obligations by partners, suppliers or customers;
- *Operational risks*: Risks occurring as a result of deviations from the internal standard processes and procedures or caused by human errors. As a rule, the source of operational risks can be found within the company;
- *Societal risks*: Risks caused by changes in the legal, political or regulatory framework and the overall situation in the society. Risk of damage to the company's reputation and image falls under this category;
- *Major project-related risks*: Risks (financial, operational, image-related, etc.) caused by the fact that one or more major projects affect the entire company and its budget.

Many companies consider all risks related to major projects to be operational risks. In this case, no distinction is being made as to the role the company plays in the project (supplier or customer; project business is a core business or not). Such approach may encounter some difficulties in case of large-scale international projects, since the category of «operational risks» as defined above does not include the totality of risks related to major projects. This applies especially to companies for which projects do not constitute their core business and therefore do not belong to the daily operations. For companies carrying out large projects occasionally, sometimes as a buyer of turnkey projects, it is advisable to use a separate risk category, that of major project-related risks. In such cases implementing a special major project risk management process may prove most helpful. Risk management would then be organised within the operational divisions involved. The reporting line for major project risk management may be suggested as follows:

Figure 41: Risk Reporting Line of a Major Project



3. Project Management Handbook

Project Management Handbook represents another risk management tool.¹⁴⁶ It provides specific instructions with respect to the rules of company's risk management process, the reporting and controlling processes for major projects in accordance with Risk Management Guidelines and Reporting Guidelines for Major Projects (if any).

Depending on the size and business model of the company, different management structures may be responsible for issuing Project Management Handbook. If the company's core business is project management, the Management Board and/or the Board of Directors are in charge.

4. Project Credit Demand Report to the Board of Directors

There are various ways how decision-making for large or major projects is organised at the Board of Directors' level in modern companies and institutions. An attempt to describe all of them would definitely overstretch the scope of this section. The process leading to a well-founded decision on whether to embark upon a large or major project constitutes one of the most important phases of project risk management. Once the decision is taken and the project is initiated, the company becomes exposed to all project-related risks, both the obvious and undetected ones.

Decision-making is basically about weighting opportunities against risks. The participants in this process are driven by different factors. So, those responsible for operational management – and willing to get started with the project – tend to underestimate its risks or to overestimate its advantages when presenting it to the Board. It is at this critical phase that only limited or vague information on risks is often being provided in the project documentation. Even if a special chapter on risks is included into the credit demand documentation, it is often being reduced to some «standard risks» lists not adapted to the specific situation of the project.

First-hand experience obtained from a number of major projects in power industry shows that risks associated with specific projects (and faced by the companies during the project cycle) tend to be underestimated and some-

¹⁴⁶ DANS (Data Archiving and Networked Services) (2006)

times not even mentioned in the credit demand documentation. Although it is impossible to foresee and exactly evaluate all the risks of a major project from the very beginning, critical assessment of project-related risks is part and parcel of project business and needs to be performed at every level of company management. Blind reliance on third-party judgements is not an option.

The reporting line on major project credit demands may be organised as follows:

Figure 42: Reporting Line of a Credit Demand Report for a Major Project



At all stages of this process main company functions (e.g. Risk Management, financial management, legal management) need to be represented.

For the purposes of decision-making, the Board of Directors should use inputs of all relevant bodies such as the financial council, legal council, risk council, technical council or other whenever required, in order for the decisions to be participative and balanced.

Some companies use the so-called «gate review process» for larger investments and major projects. Gate review process, usually consisting of three to six “gates”, requires that the investment credit demand report undergoes different stages of reporting at operational management level before eventually being presented to the Board of Directors (if needed). The stages correspond to different degrees of detail presented in the project credit demand. Such approach is particularly instrumental if substantial investments are involved during the preparation phase or extensive negotiations with partners or customers are necessary.

Gate review process offers the advantage of tight control and constant information, whereby the management board follows all the development of the credit demand report.

It also gives a possibility to stop the project at any stage of the process with minor or moderate losses if some of the conditions are not fulfilled.

The major disadvantage of this method, especially for large and complex companies, is that it might be very time-consuming. Gate review process, for instance, is not suitable for assessing short-term opportunities on the emerging markets when a quick reaction time is required. Therefore, the management and Board of Directors should carefully evaluate arguments in favour or against using a specific process, as well as the areas of its implementation.

Risk-related part of a major project credit demand report¹⁴⁷ should include the main elements as follows:

- Major risks;
- Risk probability;
- Options for taking mitigation action.

Major risks

This part of the credit demand report should reflect the most important risks of a major project such as:

- Project financial risks;
- Project time schedule risks;
- Risks related to delivery in terms of scope and quality;
- Contractual risks.

as well as general risks, i.e. those concerning not only the project but the whole company (see section 2):

- Market risks;
- Counterpart-related risks;
- Operational risks;
- Societal risks.

147 Cf. Department of Treasury and Finance (2004); DANS (Data Archiving and Networked Services) (2006)

Risk probability

Experts perform assessment of risk probability, and ideally experts involved in such assessment should represent different areas of the company's activities, and not only the project team.

Options for taking action

In order for the decision of the Board of Directors to be informed and balanced it is important that the entirety of company options be analysed during the start-up phase. In practice, solutions offered and supported by individual departments are often biased by the specificity of those departments and do not sufficiently take into account other interests. The best option from the technical point of view does not necessarily offer the best business opportunities for the company or company group as a whole. The choice of the Board of Directors should therefore be based on the complete picture: all feasible options for action should be considered. Whenever analysis and comparisons have taken place at an earlier stage, the Board of Directors should be informed of the conclusions prior to taking decision on the course of action to follow.

5. Final Major Project Credit Demand Report (closing of Internal Credit Line)

After finishing all activities and closing the internal accounts of a major project, a final status report should be presented to the Board of Directors. Final status report should be issued no later than one year upon the completion of the major project activities. The final report should have the same format as the initial credit demand report and its contents should be standardised to facilitate the assessment of the project by the management board and the Board of Directors. The report should present information on the overall success of the project and provide details on its individual aspects. At this stage, information on lessons learnt becomes most valuable. It should be disseminated to all other project managers of the company group to inform them about the specific lessons from the project and to introduce mitigation measures in other projects, if necessary, or to avoid the same or similar problems or mistakes in other projects.

For practical purposes, the final major project credit demand report should include at least the following elements:

- Name of the project;
- Registration number and date of the initial major project credit demand report;
- Summary by the project manager describing the main tasks of the project and their achievement;
- Detailed results (major goals achieved/not achieved, if latter, why);
- Time schedule (deviations from the time schedule, where and why);
- Presentation of the closing account of the project (overflow or not), including exchange rate effects;
- If the project has a cost overflow, a detailed description should be presented;
- Lessons learnt.

With the approval of the final major project credit demand report by the Board of Directors, the project is considered closed.

6. Reporting of Major Projects to the Board of Directors (Guidelines)

One of the key elements of risk management in major projects is the organisation of the reporting process to the management board and the Board of Directors.

The goal of reporting consists in informing the management board and the Board of Directors on the status of selected major projects at least every three months (quarterly report). It is recommended to use a uniform reporting template allowing the Board of Directors to identify changes in the performance of major projects easily and to initiate corrective and mitigation actions, if necessary.

a) Definition of a Major Project

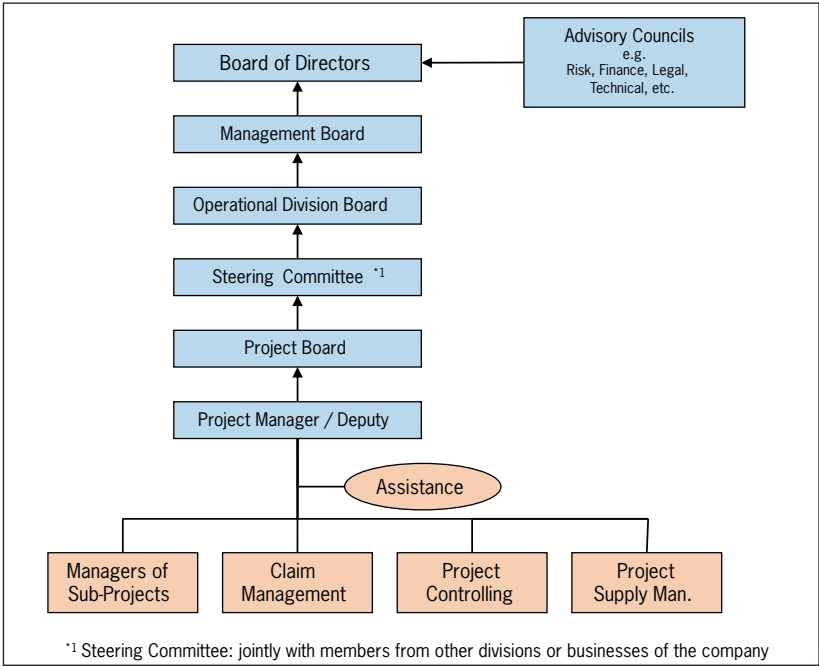
A project is considered «major» if it has strategic importance for the company. The criteria to be fulfilled for a project to fall under this category depend very much on the management policy and the nature of the company business. A

non-exhaustive list of general criteria is given below:¹⁴⁸

- The project has high financial impact on the company;
- The project can create a substantial reputation risk to the company;
- The project is of outmost importance for the development of the company or its business and/or its product line and strategy.

This section does not provide a detailed description of the organisational structure of a major project. In any case, smooth interaction with the operational management and the Board of Directors depends very much on the project manager. Appointing the right person to this position is therefore of key importance. Whatever organisational structure is selected for the project, it should provide for a minimal reporting line.

Figure 43: Example of the Organisational Structure of a Major Project



148 Cf. Department of Treasury and Finance (2004); PWC (2008); Meredith and Mantel (2011)

b) Standard Major Project Report to the Board of Directors

The company department responsible for overall reporting (*either the business development department or the group risk manager*) initiates quarterly reporting on major projects. Operational divisions prepare reports and present them to the management board and the Board of Directors. Practical experience and various publications suggest that quarterly major project reports should have a standardised form, for better efficiency.

A one- to two-page report shall contain the following minimum information:

- Overall status of the major project;
- Time schedule presented as a trend diagram;
- Project cost development (credit, current cash out and committed cash out, forecast for project costs until completion);
- Risks and opportunities;
- Summary

In general, individual elements of the report should be presented according to the following criteria:

Overall status of the major project:

The overall status of the project can be presented in a qualitative way, e.g. using a «traffic lights» system to assess such aspects as time schedule, project costs, fulfilment of project goals, situation in terms of resources (manpower) and, last but not least, risks.

Colour code:

- **green:** no significant discrepancies are observed or forecast between the original planning and goals and the current status of the project (it is up to the company to define what should be considered a «significant deviation»);
- **yellow:** some medium-scale deviations from the original planning and goals of the project are already observed or expected. The deviations are not alarming. However, they need more attention on behalf of the management (the company gives its definition of medium-scale deviations);

- **red:** greater deviations from the original planning and goals of the project can already be perceived or are expected. The project needs special attention from the management. Without clearly defined mitigation actions the goals of the project will be missed (the company should define what greater deviations are).

Time schedule trend diagram:

Time schedule trend diagram shows overall current situation of the project (delays; delivery ahead of schedule), and presents a forecast.

Development of project cost (in comparison to credit and budget):

Project cost is divided into external and internal costs (credit in comparison to already paid and committed cost – deviation of the total cost to the credit). The forecast for the final cost of the project should be included.

Risks and opportunities:

Project manager should provide a list of the most important risks within the project and relevant to the company as a whole. They should assess the pertinence of the identified risks. Furthermore, project manager reports about all claims against the company, the respective counterclaims and the development of the contingencies. It is equally the project manager's duty to present project-related potential opportunities.

Summary:

In the summary part project manager gives a short description of past and future project milestones, providing an outlook. Furthermore, project manager explains the reasons for significant deviations in project fulfillment (yellow or red lights in the overall status chart). Finally, project manager presents an overall analysis of project status, stating its major achievements and challenges.

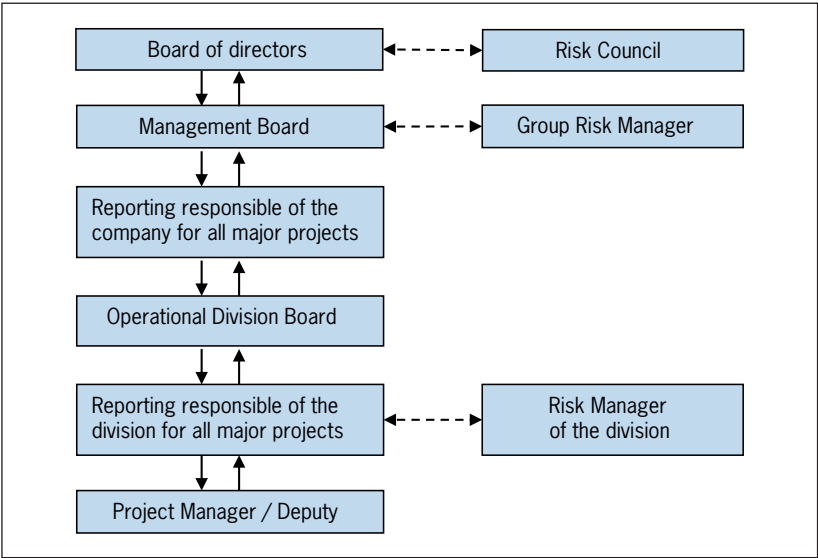
Before the report is handed over to the management board and the Board of Directors, the person in charge of company reporting clarifies open points and questions with his or her counterparts in the operational divisions. Thereupon, the head of the division releases the project report. If the person

responsible for the overall company reporting is not the group risk manager, the report should first be submitted to her/him for comments, and only after that released to the managers of the operational divisions.

The management board studies the project report and presents it to the Board of Directors for further examination. All actions identified in the course of reporting are communicated according to the previously defined modalities to the person responsible for the company group reporting and to the operational divisions. The totality of suggested actions is analysed with the support of the division managers, and relevant steps are then initiated.

The reporting on a standard major project may be organised as follows:

Figure 44: Organisation of a Standard Major Project Report (Reporting Line)



If the company is involved in more than ten major projects, it appears useful to prepare a brief overview for the Board of Directors and submit it along with the major project report. Based on this overview, the Board can decide which of the projects needs more attention at board level, and on which more

information should be provided. Every project listed should be represented by just one line containing the absolute minimum on information, namely:

- Name of the project;
- Short description of the content;
- Overall status (again, with a «traffic lights» system: green, yellow, red);
- Overall credit sum (including additional credits);
- Number of additional credits;
- Cash out and committed cash out;
- Forecast of total project costs until its completion;
- Deviation from the total credit, given as percentage (could be illustrated by selecting a corresponding colour for the respective field; «traffic lights» system);
- Key measures (illustrated with the «traffic lights» system: green, yellow, red);
 - ▷ Cost
 - ▷ Time schedule
 - ▷ Goals
 - ▷ risks
- Remarks (here, in particular, a short explanation for yellow and red lights).

7. Aggregated Risks of a Company in Relation to Major Projects

It is important to distinguish between the risks related to a major project and the aggregated risks of the whole company, resulting from the sum of influences the company is exposed to, major projects being only a part. Project risks are described in detail in the major project reports provided by the project manager to the operational division, the management board and the Board of Directors. The aggregated risks need to be presented in an overall risk report of the group risk manager to the Board of Directors, issued at least once a year, a better option being every six months (see Group Risk Report section below). Aggregated risks are handled in a different way than single major project risks; they are linked to such parameters as total risk exposure and risk appetite of a company.

a) Group Risk Report to the Board of Directors

The group risk report is a document issued by the group risk manager at least once a year; a more frequent issuance – for example, every six months – is advisable. Its minimum requirements in terms of content should include the following:¹⁴⁹

- Summary;
- Description of the major risks the company faces;
- Overview of major financial figures and their dynamics based on different scenarios;
- Development of the risk exposure of the company (risk appetite and risk reserve);
- Risk chart for all major risks (see also Chapter IV, Figure 21);
- Major damaging events during the last reporting period;
- List of all major risks of the company (risk inventory).

b) Risk Inventory

Risk inventory is issued under the leadership of the group risk manager, jointly by the risk managers at the group level and by the operational divisions, at least once a year. The inventory should include the totality of all detected risks in terms of financial exposure, reputation risk, market risks and specific project-related risks.

c) Risk Inventory for Major Projects

Risk inventories are basically lists of risks adapted to the specific nature of the project in question; they are linked to the requirements and expectations of the Board of Directors. Although there are no strict recommendations as to the number of risks to be assessed or to the exact content of such an inventory, every risk listed should be accompanied by the following details:¹⁵⁰

- Name of the company manager responsible for the project;
- Name of the manager responsible for risks;
- Short risk description – it is advisable to include information on:

149 Cf. Sanches (2005); Caltrans (2012); Sadgrove (2005)

150 Cf. Caltrans (2012); Internal Guideline of Axpo Holding; Sadgrove (2005); Camilleri (2011)

- ▷ risk of non-delivery by one or more major suppliers;
- ▷ risk of delays and postponing;
- ▷ risks resulting from interaction with other projects, or other relevant details.
- Relevant key figures of the company (e.g. EBIT) that are being at risk as a consequence of major project;
- Risk probability;
- Total risk exposure (all risk positions of a major project constituting a financial threat);
- Risk probability and total risk exposure for the last reporting period;
- Description of the changes which may transform the risks.

To facilitate comparisons, it is advisable to accompany each risk position listed in the group risk report with a graph showing the current results against those of the previous period as described in Chapter IV, Figure 21.

8. Communication in Major Projects

Among other risks related to major projects it is important to highlight the risk of damage to the company's reputation. This category of risks is of particular relevance for projects that increase the company's exposure to the public opinion – either because of the large scale of such projects or when the project is sensitive or entails serious consequences for the public at large. For such projects, it is of utmost importance that a proactive approach is adopted, and that a holistic information and communication strategy be developed and timely implemented.

The main elements of such strategy are:¹⁵¹

- a) providing information to the public stakeholders immediately involved, e.g. by organising information events for the local and municipal authorities, on a regular basis;
- b) providing information to the media on the important milestones of the project (a first press conference or a similar event needs to be organised before starting the project);
- c) informing both public and media about possible delays in the project or

¹⁵¹ Mazzei and Scuppa (2006)

any other major deviations, should such delays and/or deviations be of relevance for the public.

Crisis communication that is organised according to specific rules is not covered in this section.

9. External Risks for Major Projects

Some of the risks a company might be exposed to often cannot be revealed by means of internal risk management processes. Lists of risk categories including market risks, counterpart-related risks, operational, societal and major project risks (described in section 2.e) often happen to omit another important class of risks – that of natural and technical disasters. Being a serious threat to the company's activities, such risks may jeopardise its survival.¹⁵² It goes without saying that this category of risks represents a significant influence factor for major projects both in the company's home country and abroad.

The latest and the best-known example is the one of Japanese nuclear power stations with respect to the risk of flood and tsunamis. The catastrophe in Fukushima followed by the bankruptcy of Tepco that used to be the world largest power producer were direct consequences of risk underestimation. Although Japanese nuclear power plant operators abided by country laws and regulations they largely ignored the evidence that according to new risk assessment methods, risk exposure of tsunamis may be higher than admitted previously (It should be mentioned that this knowledge had already been recognised by a wide number of nuclear power plants across the world).¹⁵³

Another example is the probability of disease outbreaks (example: swine flu in 2009) or the reliability of power supply in a specific country.

This illustrates clearly the necessity to increase risk preparedness of a company well in advance, before embarking on large projects and investments.

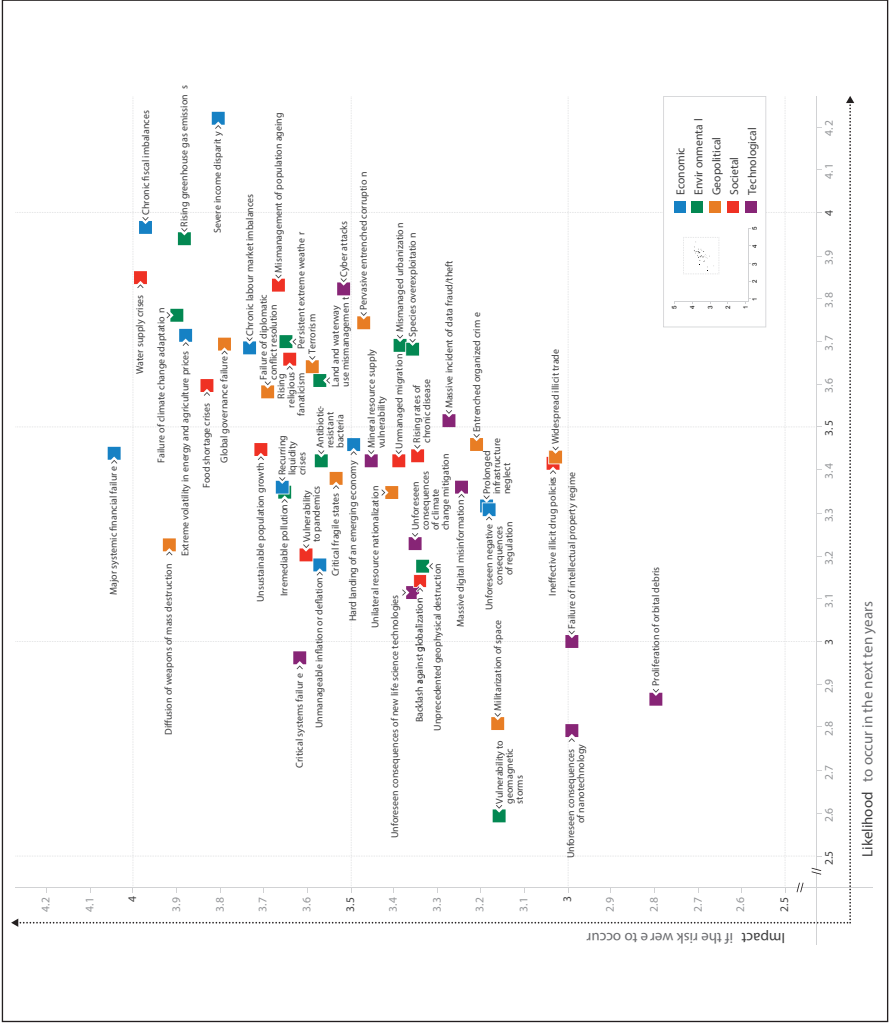
Risk report of the World Economic Forum 2008¹⁵⁴ gives an example of an external expert source used for conceiving and implementing such preparedness measures.

¹⁵² Sanches (2005)

¹⁵³ www.ensi.ch; ENSI-AN-7614, 7669, 7746, 7800; Fukushima Berichte (The Fukushima Reports); 2011

¹⁵⁴ WEF (2008)

Figure 45: The Global Risks Landscape 2013¹⁵⁵



Source: WEF (2013: 53)

155 WEF (2013:5)

10. Decision-making to Minimise or Mitigate Risk of major Projects

The more complex the company processes are, the more people are involved in decision-taking phases of major projects. In a multidisciplinary project, it is often necessary to ensure that all the disciplines involved are represented in order to assess the consequences of a potential decision for all the stakeholders and for the project as a whole, as clearly as possible. Such assessment task is what the company management and boards are faced with. In fulfilling this task, it is crucial that they follow a structured, balanced and careful approach. Having a set of standard and exactly defined procedures helps to reduce the risk of hasty solutions and avoid dominators.

As a rule, it is not by following some intended trajectory or by implementing the most obvious option alone that sustainable solutions and, consequently, a significant risk reduction can be obtained, but rather by carefully weighing and comparing all relevant possibilities.

It is precisely by concentrating on the detection of possible errors and sources of errors that HROs (High Reliability Organisations) – such as aircraft carriers, nuclear power plants or air traffic control systems, to name just a few – achieve an extremely low rate of failures. This means that the employees of these organisations have to concentrate on something they are rarely faced with. Such approach translates into frequent analysis of incidents, accompanied by careful reporting of all failures, however minor these may appear, and an almost obsessive focus of the members of staff on the downside of success¹⁵⁶. This phenomenon is observed at all levels of HROs' hierarchy up to the management and the Board of Directors.

There are different techniques of systematic decision-finding. The one presented below stems from the field of HROs and is used fairly frequently: FO²RDEC (see Appendix 8).

Yet before the decision-finding process is discussed in detail, it is necessary to consider another important cultural element that constitutes a prerequisite of any decision-making. Analysis of incidents, errors and potentials for improvement can only be possible if such events are duly reported.

¹⁵⁶ Weick/ Sutcliffe (2003)

Practical experience shows that members of staff need to feel confident if they are to report irregularities. If they fear sanctions, they would rather ignore or cover up failures, possible errors or technical problems. At the same time, actions by company management, its directors and board that motivate the employees to ask questions and uncover errors or failures strengthen an organisational culture that values failure reporting and strives to avoid errors in the future.

Cultural aspects cited above are just as important for minimising risks in major projects and organisations as any technical know-how or technology; furthermore, they constitute one of the key prerequisites for a functioning FO²RDEC¹⁵⁷ analysis, the latter being based on confidence.

157 Cf. Hörmann (1994); Hörmann (1995: 17-23)

VIII. Summary and Guidance for Practice

1. Summary

a) Key Messages

The role of the Board of Directors (BoD) to define the strategic direction for the enterprise has been well established in Corporate Governance. In Switzerland, it is even stipulated by law. The Board of Directors (BoD) has to balance the opportunities and risks that the company faces in formulating and developing those strategies with an enterprise-wide perspective. This role has gained great importance in recent years, especially in large multinational corporations, for the following – not exclusive list of – reasons or events: Increased uncertainty and volatility in the global business environment, financial crisis of 2008, corporate scandals, natural and manmade catastrophes, terrorism, shareholder activism, legislations like Sarbanes Oxley (US), Too big To Fail regulations (CH – FINMA), clout of large pension funds due to high investment volume. The factors mentioned had a lasting effect on the perception of risk and the attitude towards risk. The failure to manage risks and to achieve envisaged objectives has far-reaching and disastrous consequences for all shareholders and stakeholders.

In this book, the authors have put forward some important messages with regard to Risk Management defined and guided by board members, including:

- The tone of Risk Management is set at the Board of Directors (BoD) and Executive Board (ExB) level;
- Surprise is a key element of risk; managing risk is managing surprise. Surprise can be managed only through maintaining strategic reserves;
- Identifying risks involving large surprises requires creativity, an open and transparent culture and an enterprise-wide participation of employees. It should not be the domain of the select few;

- The Failure Mode and Effect Analysis (FMEA) approach, based on workshops and democratic decision-making, can be used for successful ERM;
- Risk Management is a process that should integrate the key functions of an organisation, including the strategic direction and control function, Risk Management Compliance Management system (CMS) and internal/external auditing;
- Uncontrollable risks, fraud and corruption risks and risks of significant projects have gained much attention in the recent years, and companies are advised to be prepared to manage those with more rigour.

b) Organisation at Board Level

The definition of the risk strategy as a part of strategic Risk Management falls entirely within the scope of the Board of Directors (BoD). The Board of Directors (BoD) should regularly provide Risk Management officers with guidelines for education and further training. It is recommended that the implementation of Risk Management should be defined and structured with organisational regulations.

If there is a special Risk Management Committee, its task ought to be guided by specific regulations. The decision to delegate some responsibilities to the Executive Board (as far as the law allows) must be clearly recorded in the minutes of a board meeting. It might be necessary to separate the duties of the Risk Management Committees from those of the Audit Committee. The latter deals amongst others with loan risks, customer creditworthiness or insurance risks. (Appendix 11 provides an example of an Insurance checklist for BoD).

Risks in connection with substitution and recruiting planning should be assigned to the Nomination Committee. It is worthwhile to define these tasks in the organisation regulations to keep them separate of each other.

The Risk Management function should closely cooperate with the internal auditing function to receive a feedback of its activities at an early stage. Therefore, the Board of Directors (BoD) has to make arrangements, if necessary, to ensure collaboration between Risk Management and internal audit officers.

c) Organisation at the Management Level

On the management level, the first step must be to determine a responsible person in charge of Risk Management. This person can be called Risk Man-

agement Coordinator or Chief Risk Officer (CRO in analogy to CEO and CFO). The responsibility of a Risk Management Coordinator or CRO has to be clearly specified, so as not to convey the wrong impression that the members of the Executive Board are no longer responsible for the risks of the company. For the CEO and Divisional Directors are, and will remain the Risk Owners or ultimate responsible for risk and its consequences. They know their business and the risks involved best. Therefore, they have to make every effort to prevent or minimise these risks.

d) Risk Management in the Company

In a company that is part of a holding, the Board of Directors (BoD) of the holding decides whether Risk Management should be coordinated and driven on company level or on holding level. Even if the Risk Management Committee and the CRO are at holding level, the affiliated companies remain responsible for Risk Management, just like the company's chief manager will remain a Risk Owner.

To make co-ordination efficient and meaningful, the following synergies can be used:

- Process standardisation;
- Form standardisation;
- Report standardisation;
- Construction of group-specific Master Risk lists;
- Premium privilege by group insurance;
- Exchange of experience among the responsible persons;
- Concentrated training and continuing education.

e) Managing Uncontrollable Risks

Uncertainty and complexity in the context of Risk Management require a board to seek new paradigms or frameworks, especially as global shocks and unfathomable risk events are increasing. The conceptualisation of uncontrollable risks is one possible framework to address the exogenous and systemic nature of risks from such events. After assessing and defining what uncontrollable risks the company faces, the board should take the initiative to evaluate jointly with management:

- Impact of diversity and of cognitive biases at the board and management level, so as to identify accurately the risks and opportunities that emerge from a uncertain and complex environment;
- Methods for the board to grasp and envision unthinkable or extreme risks (black swans) in the context of the existing risk landscape and Risk Management practices such as risk scanning and risk master lists;
- Influence of «complexity science» as a conceptual framework for the board's evaluation of risk maps – i.e. considering «systems thinking» to explore the linkages across risks identified to assess or hypothesize intersecting vulnerabilities and possible cascading consequences.

After identification and visualisation of possible risk clusters, the board and management should consider possible risk contingencies or scenarios, both from a corporate Risk Management and business continuity management perspective.

f) Managing Fraud and Corruption Risk

Fraud and corruption risks can take many shapes, varying from gifts and entertainment via facilitation payments, bribes, kickbacks and overbilling schemes to the use of (rogue) agents and charitable contributions. Fraud and corruption risks are a business reality and are often underestimated (on purpose or not) by European companies. Tighter regulations and stricter enforcement, however, will mandate companies to deal with these risks instead of looking away. For the board and senior management the challenge will be to set the right tone and lead by example. Employees need to understand the rules and need to know how to apply them, but they also have to feel comfortable to seek guidance or report misconduct without fear of retaliation. This requires management to foster a culture that allows or encourages such behaviour. It also implies a reappraisal of the target setting, performance measurement and incentive systems.

g) Risk Management of Major Projects

Since every project involves its specific risks, it is almost an obligation to do Risk Management at the project level, though of course depending on the pro-

ject size. Not surprisingly, it is common practice in companies with well-developed project management processes. Yet there are cases when a project as such puts the entire company at risk, either because of the scale of the investments involved or due to a significant exposure of the company reputation. Such projects must be part of the overall company Risk Management, and the Board of Directors should receive reports on them and deal with them on a regular basis. Oddly enough such projects are often perceived as not falling into the competence of the Board of Directors. It should be added that the public sector, i.e. governmental or regional organisations, issue a substantial share of large projects, often underestimating the importance of professional project management and risk control.

Numerous examples from the history of project management demonstrate quite clearly how projects can expose the entire company to a major risk or even lead to its bankruptcy.

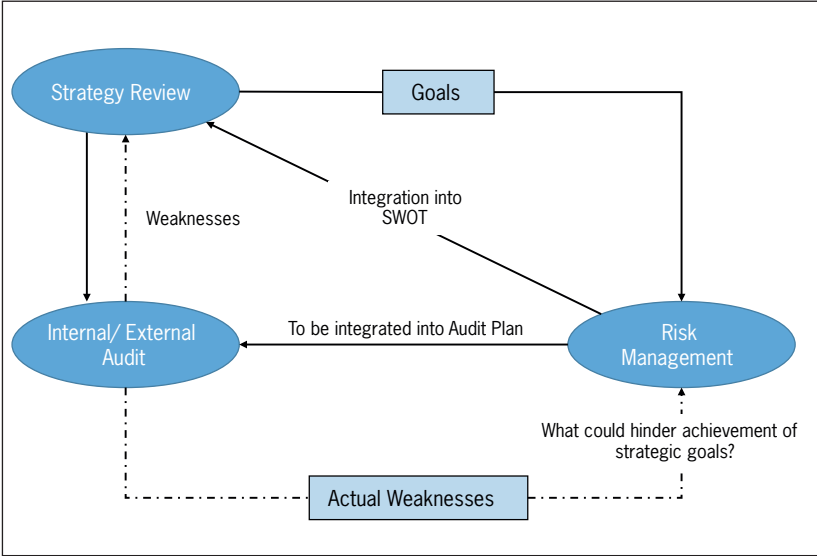
2. Risk Management Practice Today

a) Integrated ERM

The Risk Management process should be integrated into the internal and external audit and strategy process and framework. The objectives are transmitted through the strategy into the Risk Management process; the results of the risk considerations in turn do not only influence the priorities of the audit plan, but also have an impact on the SWOT analysis in the strategy process¹⁵⁸ (see Figure 46).

¹⁵⁸ Boutellier and Kalia (2006)

Figure 46: Integrated Risk Management



Source: Boutellier and Kalia (2006)

One of the important ways to reinforce the link between strategy and Risk Management is to have a feedback loop from the Risk Management function to the strategy function. This is normally not the case, and if so, this occurs implicitly through reporting mechanisms. Doing so, however, reveals the status of risks and how Risk Management has performed in terms of achieving strategic objectives. Such a process would, for example, facilitate integrating information from the subsidiaries and divisions into the next strategy and Risk Management cycle. A brief proposal from the Risk Management function to the strategy implementation function could serve as a starting point for the next strategy implementation cycle. Such risk feedback from the subsidiaries may have major implications for the strategy process.

The concept of risk assessment and feedback over different levels of management is also embodied in the concept «3 Lines of Defence» which is very common in the financial sector.

- 1st Line of Defence: Management with its day to day management of risks;
- 2nd Line of Defence: Independent control functions (reporting lines to senior management) that monitor if risks are managed adequately and in line with policies and frameworks by the 1st line of defence;
- 3rd Line of Defence: Internal and external audit function reviewing the quality of Risk Management by the 1st and 2nd line of defence; reporting directly to the BoD (with complete independence from management).

b) Decision-Making Under Time Pressure

Risk Management is never complete, as new and unidentified risks keep emerging. Once the risk indicator or risk event occur, the critical success factor is optimising decision-making under time pressure. This area of Risk Management is being embraced by the term Business Continuity Management (BCM).¹⁵⁹ Statistics seem to indicate that 70 % of businesses go bankrupt when facing disasters such as fire. Thus the success of Risk Management is not warranted by managing a few selected strategic risks, but also unexpected risks and crises. Goldman Sachs is a well-known case for illustration. When the September 11, 2001 terror attacks in New York occurred, the company's offices were just two blocks away from the high impact zone. Due to a good concept for such an event, its operations went on without any disruption, with the employees working from hotel rooms and/or with personal notebooks.¹⁶⁰ BCM is a crucial step to mature Risk Management in a company, but at an advanced stage Risk Management is embedded in Business Continuity Management. Optimal decision-making in crisis situations demands the following prerequisites:

- Experience;
- Regular training;
- Projects;
- Processes;
- Transparency.

¹⁵⁹ See Section (I.4.a)

¹⁶⁰ Economist (May 2006)

c) Whistleblowing

As explained by Kimmich,¹⁶¹ a «whistleblower» is a person who figuratively stands up amidst an event and, figuratively, blows the whistle, thereby attracting everyone's attention with the intention of stopping what is going on. The whistleblower reports alleged corporate misconduct and the process is termed «whistleblowing». The US have enacted several laws to encourage whistleblowing so that impending threats or failures can be identified earlier and damage can be minimised in good time.¹⁶² The laws introduced aim to safeguard whistleblowers against discrimination and harassment by perpetrators or persons in power positions.

The impact of US legislations has had global impact. In Switzerland, too, some companies have accepted the benefit of whistleblowing and have started to integrate it. It is advisable that Swiss companies pay close attention to this subject and initiate formal whistleblowing policies, especially in large publicly listed companies. Appendix 6 shows the whistleblowing policy document adapted from a leading Swiss company.

d) Checklists

Checklists are a very effective tool to monitor Risk Management. Board members may benefit considerably if they get periodically updated checklists related to the key risks. Checklists, for example, could be related IT-risks, contract risks, succession planning and key personnel risks as well as hazard risks. Such lists, however, have to be based on real groundwork undertaken by managers; otherwise there is a danger that they might just become a tick-box exercise and provide false assurance to the Board of Directors (BoD) and shareholders that everything in the company is under control. The board members should make random spot checks and conduct independent investigations to verify the accuracy of these checklists.

An anonymised example of an IT-risks questionnaire of a leading high-tech company in Switzerland is provided in Appendix 5.

¹⁶¹ Kimmich (2006: 52)

¹⁶² Sarbanes Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745

e) Small and Medium Companies

Large enterprises today have resources, intent and pressure to implement and document Risk Management as discussed above. However, it is not the same for small and medium companies. Therefore, the level of requirements for such companies should be facilitated adequately, e.g. by collecting information about the company's risks from interviews, from management or board meetings. This may become critical in the case of small and medium companies. A certain level of highly recommended/ mandatory (◆) and optional components (○) as demonstrated in the following Table 8 should be expected in today's future-oriented companies.

Table 8: Essentials of Enterprise Risk Management for Different Scale Companies

Key Components/ Enablers	Large Firms	SME	Small Firms
Objectives	◆	◆	◆
Policy	◆	◆	○
Guidelines/ Directives handbook	◆	○	
Structures			
Formal Organisation	◆	○	
Informal Organisation		◆	○
Roles			
Dedicated RM Roles	◆		
Additional RM Roles		◆	○
Process			
Formal	◆	◆	
Informal			○
Reporting			
Formal	◆	◆	
Informal			◆
Communication			
Formal	◆	◆	○
Informal	◆	◆	◆

Key Components/ Enablers	Large Firms	SME	Small Firms
Culture			
Training, Educational Seminars	◆	○	○
Awareness	◆	◆	◆
Tools			
MIS Tools	◆	○	
Quantification and Statistical Tools	○	○	○

This issue can be further illustrated by an example of a medium-sized company in the food industry in Germany. Under the KontraG requirements, the company had to implement a formal Risk Management to which the board members took a very pragmatic approach.

First of all, instead of a standard classification, the company made a very simple classification, which is easy to understand in the company-specific situation. The key risks were classified into four main categories:

- Safety regarding food (strategic risks);
- Safety regarding production facilities (Health, safety, security);
- Crisis Management (Business Continuity Management);
- Operational Risks (Finance, HR, Machinery).

Moreover, a personal approach was adopted to collecting risks rather than running workshops or circulating questionnaires. This company provides a good example of how Risk Management can be suitable for all companies at all levels – without becoming a complex and resource-consuming exercise.

f) Managing Impediments

The decision to establish Enterprise Risk Management is a big decision and needs the complete and unwavering support of the board and Executive Board (ExB). This is important as there are several impediments to establishing ERM which the boards and Executive Board (ExB) should be aware of before the process is started. They should be well prepared for managing these impediments as they pose a risk to establishing Risk Management in the organisation. Some of the common impediments are:

Short sightedness: Risk Management has a future orientation. There will be some board-members or members of management who could be short-sighted and therefore focused on immediate concerns or have no inclination to focus on a long-term initiative with no tangible benefits in sight.

Different priorities: Risk Management might not be at the same priority level for all the key decision-makers.

Misconception about the role: Some Board members believe that Risk Management is either the role of the internal auditing or finance department. This could be true in some particular situations. However, auditing has a past orientation and Risk Management has a future orientation. This difference has to be clear irrespective of who is responsible for managing risk. Secondly, enterprise Risk Management goes beyond financial Risk Management. Today, finance is just one part of Risk Management.

Lack of awareness and management buy-in: Owing to the reasons cited above, the major challenge for organisations today is that of management buy-in. If that occurs on a large scale, Risk Management just becomes a formality.

Change process: Change is always resisted. For Risk Management to be «lived», it needs at times unpopular or courageous ideas, such as increased transparency, future orientation, creative and unconventional solutions or democratic decision-making. This demands tough decision-making as well as dealing with complexity arising from change. Serious commitment, focus and time are expected to initiate changes – which is not always easy.

Overlaps and power struggles: There are many overlaps that can occur as it is difficult to separate the responsibilities of boards, Executive Board (ExB) or other participants. Risk Management requires some high-profile decisions; consequently, a lot of power is vested in the persons initiating these decisions. This may lead to conflicts, to the detriment of Risk Management. Conflicts can also result from differing objectives and agendas for Risk Management by various key participants.

Competence of team members: Competent people are rare, which is also true for Risk Management, especially because the field is relatively new and very dynamic, there is still no clear acceptance of how Risk Management should work in an organisation. Companies need to make careful choices in this respect, selecting people who know the business, who know Risk Management and can influence others effectively with regard to Risk Management.

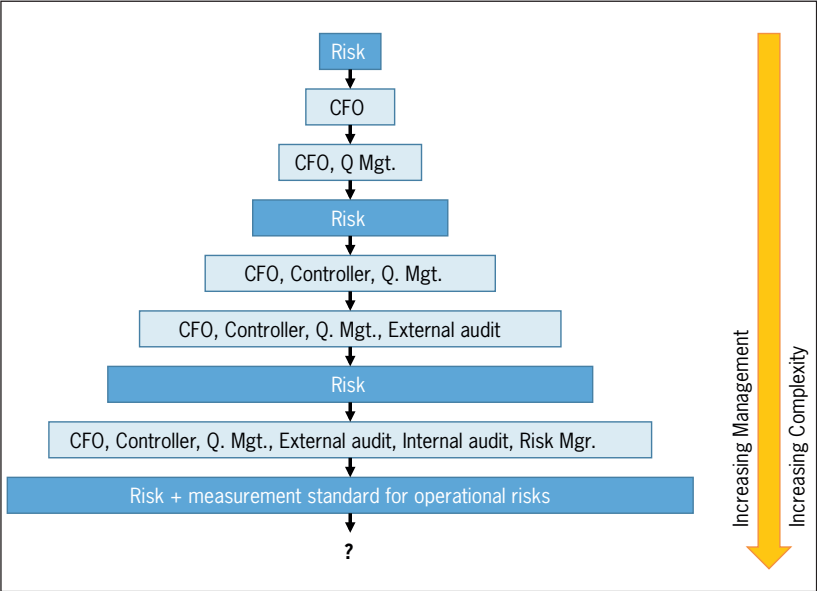
g) Self-Appraisal

Risk Management is a process and effective Risk Management calls for constant improvement. To this end, companies are advised to carry out a self-appraisal exercise at least once a year; 360° feedback is recommended for all hierarchy levels, functions, divisions and geographical locations. This provides information about the Risk Management perception of all stakeholders and all the critical elements of Risk Management, including the soft (but important) elements like culture. For a sample self-appraisal questionnaire, see Appendix 7.

h) Keep it Simple

A perceived increase in bureaucracy (or increased redundancy) is common and a very important concern for board members today. For many, Risk Management and assurance initiatives are bureaucratic additions to the organisation. The assertion is not unsubstantiated – a poorly planned implementation early in the process, or the failure to elicit management buy-in could result in a bureaucratic structure that yields little additional value for the organisation. Similarly, over-management should be avoided as it could lead to Perrow's dilemma – the higher the complexity of the system, the higher the risks it runs (see Figure 47). Figure 47 demonstrates how the back-up systems in management are making the Risk Management systems in enterprises more and more complex. These functions, moreover, have numerous interactions, making the system more complex and hence prone to higher risks.

Figure 47: Perrow's Dilemma in Management



Source: Boutellier and Kalia (2005)¹⁶³

The statement «Risk Management is an art not a science» seems true in this context.¹⁶⁴ It is likely that board members and the Executive Board (ExB) have to make conscious and determined efforts if they are to avoid the perception of Risk Management being no more than an additional bureaucratic burden. They are most likely to succeed if their actions reduce complexity and promote simple solutions.

¹⁶³ Boutellier and Kalia (2005)

¹⁶⁴ Statement by a Risk Manager at the FERMA Conference, Brussels, Belgium (October, 2004)

Epilogue

A medium-sized Swiss company situated near a lake and a small creek has established exemplary Risk Management in the last few years. One of the two identified risks were the flooding of the production unit because of the high-tide of the lake and the overflowing of the creek. After careful assessment the high-tide was considered a high-level risk and the overflowing of the creek an insignificant risk. However, the opposite happened. In 2005, floods brought a lot of water to the premises, along with logs from the uprooted trees, and stopped production. In reality, the lake never created problems. Risk assessment was obviously mistaken, but the crisis management in place and the actions planned to safeguard the production unit in case of a high tide, reduced the unrecoverable losses to a minimum. The company even resumed production in the subsequent week.

Risk Management, as described in this book, provides much advice and many insights for better and sustainable operations; it also increases stakeholder value. But it must always be remembered that Risk Management is not a remedy for everything that can go wrong in a company. Things might go wrong despite the best possible Risk Management; however, Risk Management allows companies to survive even a great storm rather than being devastated and becoming insolvent.

Bibliography

- 4N6 Factory (2014), «Fraud Risk Management Framework»
- ACFE (Association of Certified Fraud Examiners) (2014), «Report to the Nations; On Occupational Fraud and Abuse»
- Available from: http://www.ey.com/GLOBAL/content.nsf/International/Article_-_Assessing_the_Impact_of_September_11 [Accessed 28 July 2002]
- Basel Committee (Risk Management Group of the Basel Committee on Banking Supervision) (2003), «Sound Practices for the Management and Supervision of Operational Risk» [online]. Available from: <http://www.bis.org/publ/bcbs96.pdf> [Accessed 23 April 2005]
- Basel Report (1998), «Operational Risk Management», Basel Committee on banking supervision [online]. Available from: <http://www.bis.org> [Accessed 8 July 2002]
- BCI (The Business Continuity Institute) (2005), «Business Continuity and Crisis Management» [online]. Available from: <http://www.thebci.org/BCAW.htm> [Accessed 16 April 2005]
- Beswick, K. and Bloodworth, J. (2003), «Risk Mapping – Dilemmas and Solutions», Risk Management Topic Paper No. 4, Housing Corporation, London
- Boutellier, R. and Kalia, V. (2005), «Integrated Model of Enterprise Risk Management: A New Approach», Internal Publication, Technology and Innovation Management Institute, Swiss Federal Institute of Technology, Zurich
- Boutellier, R. and Kalia, V. (2006), «Risikomanagement auf Unternehmensebene: Notwendigkeit und Gestaltung», in: Oliver Gassmann, Carmen Kobe (Hrsg.): Management von Innovation und Risiko – Quantensprünge in der Entwicklung erfolgreich realisierte, 2. überarbeitete Auflage, Springer-Verlag Berlin
- Brauner, C. (2001), «Preparedness – Basics of business continuity management», Swiss Reinsurance Company, Zurich
- Cadbury Report (1992), «Report of the Committee on the Financial Aspects of Corporate Governance» [online]. Available from: <http://www.ecgn.org> [Accessed 22 June 2002]
- Caltrans (2012), «Project Risk Management Handbook: A Scalable Approach», Version 1, June 2012
- Camilleri, E. (2011), «Project Success: Critical Factors and Behaviours», Gower Publishing
- Clifford Chance and Economist Intelligence Unit (2014), «A view from the top: A board level perspective on current risks»
- CMI (The Chartered Management Institute) (2005), «Business Continuity Survey 2005» [online]. Available from: <http://www.managers> [Accessed 23 July 2002]
- COSO (The Committee of Sponsoring Organisations of the Treadway Commission) (2003), «Enterprise Risk Management Framework», July [online]. Available from: <http://www.erm.coso.org>. [Accessed 23 Mai 2004]
- Cressey, D.R. (1973), «Other People's Money», Patterson Smith, Montclair

- DANS (Data Archiving and Networked Services) (2006), «Project Management Handbook», Version 1.1 – July 2006, The Hague
- Decker, A. (2004), «Business continuity management: A model for survival» [online], White paper: business continuity. Available from: http://www.eds.com/services/innovation/downloads/business_continuity.pdf [Accessed 2 April 2005]
- Dekker, S. (2014), «Safety Differently: Human Factors for a New Era», 2nd Edition, CRC Press
- Department of Treasury and Finance (2004), «Investment Lifecycle Guidelines: #2 Project Risk Management guidelines», Version 1.0, Feb. 2004, Melbourne
- Dowd, K. (1998), «Beyond Value-at-Risk: The New Science of Risk Management», John Wiley & Sons, London
- Drennan, L. (2001), «Corporate Governance: A Mandate for Risk Management», Division of Risk, Caledonian Business School, Glasgow Caledonian University [online]. Available from: http://www.nottingham.ac.uk/business/cris/okec/2001_paper4.doc [Accessed 8 July 2002]
- Dubs, R. (2006), «Verwaltungsrats-Sitzungen: Grundlegung und Sitzungstechnik», Bern/ Stuttgart/ Wien: Haupt Verlag
- Economie Suisse (2014), «Swiss Code of Best Practices for Corporate Governance»
- EQE (2002), «Risk Management in the UK: A Board-level Priority» [online]. Available from: <http://www.eqe.com/publications/revf94/risk.html> [Accessed 8 July 2002]
- Ernst & Young (2002), «The state of the industry: Assessing the Impact of September 11» [online].
- Ernst & Young (2002a), «Verwaltungsrat und Umgang mit Risiko», WM Wirtschafts-Medien AG, Bilanz, Zürich
- Ethics Resource Center (2012), «Retaliation: when whistleblowers become victims», Supplemental Report of the 2011 National Business Ethics Survey
- Ethosfund (2005), Available from: www.ethosfund.ch [Accessed 2 September 2004]
- FATF (2012), «International Standardson Combating Money Laundering and the Financing of Terrorism & Proliferation», The FATF Recommendations
- Freedman, D.H. (2000), «Corps Business: The 30 Management Principles of the U.S. Marines», New York: HarperBusiness
- Gietl, G. and Lobinger, W. (2006), «Risikomanagement für Geschäftsprozesse: Leitfaden zur Einführung eines Risikomanagementsystems», Pocket Power, Hanser, Germany
- Giger, G. (2002), «Genügt das schweizerische Aktienrecht einer zeitgemässen Corporate Governance?», Der Schweizer Treuhänder, 5(02): 423-428
- Gindi, G. (2003), «Normen zu NORMA», Hannover, 17
- Gleissner, W. and Fuser, K. (2003), «Leitfaden Rating», 2. Aufl., München
- Gleissner, W.; Lienhard, H. and Stroeder, D. (2004), «Risikomanagement im Mittelstand, RKW-Schriftenreihe», Eschborn
- Haller, M. (1999), «The Global Development of Risks – Consequences for Integrated Risk Management», Risk Management Foundation, I-VW HSG St. Gallen
- Hampel, R. (1998), «Committee on Corporate Governance», Final Report, Gee, London
- Härtsch, N and Müller, R. (2009), «Risk Management an Hochschulen: Ein Praxishandbuch für Universitäten, Fachhochschulen und weitere Bildungsinstitutionen», Dike Verlag AG, Zürich

- Hauser, Ch. (2012), «Korruptionsrisiken erfolgreich begegnen – Strategien für international tätige Unternehmen», HTW Chur
- Hilb (2004), «Corporate Governance: gezielte Gewinnung, Honorierung und Förderung von Aufsichts- und Verwaltungsräten», Freiburg i. Br. : Haufe: 50
- Hilb, M. (2005), «New Corporate Governance – Successful Board Management Tools», Berlin et al., Springer
- Hörmann, H.-J. (1994), «Urteilsverhalten und Entscheidungsfindung», in «Effektives Arbeiten im Team: Crew Resource-Management-Training für Piloten und Fluglotsen», Deutsches Zentrum für Luft- und Raumfahrt, Hamburg
- Hörmann, H.-J. (1995), «FOR-DEC. A prescriptive model for aeronautical decision making», in «Human Factors in Aviation Operations», Proceedings of the 21 st Conference of the European Association for Aviation Psychology (EAAP) (Vol. 3) (pp. 17-23), Avebury Aviation, Aldershot Hampshire
- ICAEW (Institute of Chartered Accountants in England & Wales) (1999), «Internal Control: Guidance for Directors on the Combined Code», London: Accountancy Books
- J.P. Morgan (1995), «RiskMetrics Technical Document», Third edition, New York: Morgan Guaranty Trust Company
- Jaisli (2014), «Grundzüge eines wirksamen Compliancemanagements», SwissHoldings / Economiesuisse
- Jorion, P.H. (1996), «Value at Risk: A New Benchmark for Measuring Derivatives Risk», Irwin Professional Publishers, New York
- Jorion, P.H. (1997), «Value-at-Risk: The New Benchmark for Controlling Market Risk», Irwin, Chicago, Ill
- Kägi, T. and Pauli, R. (2003), «Risk Management und konjunkturelle Sturmwarnung», in: UBS Outlook 4/2003, Zürich, 7
- Kalia, V. (2006), «RISK MANAGEMENT AT THE BOARD LEVEL: An Empirical Study of Swiss Multinational Companies», Universität St. Gallen, Dissertation
- Kimmich, P. (2006), «Effective Corporate Compliance Programs: The impact of the 2004 Amendments to the U.S. Federal Sentencing Guidelines for Organisation», University St. Gallen, Dissertation
- King II Report (2001), «King Report on Corporate Governance for South Africa – 2001», Institute of Directors: 30-31, 67-70
- KING III (2009), «Corporate and Commercial: King Report on Governance for South Africa»
- Kloman, F. (1999), «Risk Management Milestones: 1990-1999», Risk Management Reports, 26: 12
- Labaton, S. and Oppel, R. A. Jr. (2002), «Enthusiasm Waning in Congress for Tougher Post-Enron Controls», NY Times, June 10: A1
- Lam, J. (2014), «Enterprise Risk Management – From Incentives to Control», 2nd Edition, Wiley
- Laye, J. (2002), «Avoiding Disaster: How to Keep Your Business Going When Catastrophe Strikes», Disaster Recovery Journal, Business Continuity Planning Model [online]. Available from: <http://www.drj.com/new2dr/model/bcmodel.htm> [Accessed 16 April 2005]
- Lewis, H.W. (1990), «Technological Risk», W.W. Norton and Company, New York, NY

- Liker, J. K. (2004), «The Toyota Way», Tata McGraw-Hill, New Delhi: 330
- Mazzei, L./ Scuppa, G. (2006), «The Role of Communication in Large Infrastructure: The Bumbana Hydroelectric Project in Post-Conflict Sierra Leone», World Bank Working Paper No. 84
- McCrackan, A. (2005), «Unravelling business continuity terminology» [online]. Available from: <http://www.continuitycentral.com/feature0195.htm> [Accessed 17 March 2005]
- McCrackan, A. (2005a), «Is business continuity a subset of Risk Management?» [online]. Available from: <http://www.continuitycentral.com/feature0178.htm> [Accessed 16 April 2005]
- Meredith, J.R. and Mantel S.J. (2011). «Project Management: A Managerial Approach», eighth edition
- Miller, G.P. (2014), «The Law of Governance, Risk Management, and Compliance», Wolters Kluwer Law & Business, Aspen Publishers
- Monks, R.A.G. and Minow, N. (1995), «Corporate Governance», Blackwell Publishers, Oxford, UK
- Müller, R. and Volkart, R. (2002), «Handbuch für den Verwaltungsrat: Für die professionelle Verwaltungstätigkeit», WM Wirtschafts-Medien AG, BILANZ, Zürich
- Müller, R., Lipp, L., and Plüss, A. (2014), «Der Verwaltungsrat: Ein Handbuch für Theorie und Praxis», 4. Auflage, Zürich
- Müller, R., Wittmer, A., and Drax, Ch. (2014), «Aviation Risk and Safety Management – Methods and Applications in Aviation Organisations», Springer, Zürich
- ONR 49000 (2004), «Risk Management for organisations and systems: Terms and principles»
- ONR 49002-1 (2004), «Risk Management for organisations and systems – Part 1: Guidelines for Risk Management
- Pareto. V. (1896-97), «Cours d'économie politique», 2 vols., Lausanne: Rouge
- Pfyyfer, H.-U. (2005), «What impact does SOX have on Swiss-based companies that are not listed on US exchanges?», Presented at the EUROFORUM Conference, Renaissance Zurich Hotel, Zurich
- Pritsker, M. (1997), «Evaluating value at risk methodologies», Journal of Financial Services Research, 12(2/3): 201-242
- PWC (2008), «A practical guide to risk assessment», Price Waterhouse Coopers
- RESIST (2011), «Resisting Extortion and Solicitation in International Transactions: A Company Tool for Employee Training», International Chamber of Commerce, Transparency International, United Nations Global Compact, World Economic Forum
- Rockafellar, R.T. and Uryasev, S. (2002), «Conditional value-at-risk for general loss distributions», Journal of Banking and Finance, 26(7): 1443-1471
- Roth, M. (2012), «Compliance in a nutshell», DIKE
- Ruud, F.T. and Bodenmann, J.M. (2002), «Corporate Governance in der Schweiz», Standpunkte der Verwaltungsräte von SWX-kotierten Unternehmen, Der Schweizer Treuhänder, 4: 273-282
- Sadgrove, K. (2005), «The complete guide to business Risk Management», second edition; Gower Publishing Company

- Sanches, P.M. (2005), «Neuronal Risk Assessment System for Construction Projects», expert Verlag
- Sanyal, R. (2005), «Journal of Business Ethics»; Volume 59, Springer, Determinants of Bribery in International Business, The Cultural and Economic Factors
- Smith, D.J. (2002), «Business Continuity Management – Good Practice Guidelines», The Business Continuity Institute [online]. Available from: <http://www.thebci.org/BCIGPG2005.pdf> [Accessed 17 March 2005]
- SOX (Sarbanes Oxley Act) (2002), One Hundred Seventh Congress of the United States of America [online]. Available from: <http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf>
- Surowiecki, J. (2004), «The wisdom of crowds». New York: Doubleday
- The Combined Code on Corporate Governance (2003) [online]. Available from: http://www.fsa.gov.uk/pubs/ukla/lr_comcode2003.pdf [Accessed 25 June 2004]
- The Network Inc. (2013), «2013 Corporate Governance and Compliance Hotline Benchmarking Report»
- The Turnbull Report (1999), «Internal Control Guidance for Directors on the Combined Code», The Institute of Chartered Accountants in England & Wales [online]. Available from: <http://www.tolsonmessenger.co.uk/resource/faqs/turnbull.htm> [Accessed 8 July 2002]
- Ullberg, E.; Rodriguez, E. and Stormby, N. (2002), «Risk Management: From Portfolio Strategy to Value – creating Systems Strategy», Geneva Papers on Risk and Insurance – Issues and Practice, July, 27(3): 467
- WEF (World Economic Forum) (2008), «Global Risks 2008: A Global Risk Network Report»
- Weick, K.E. and Sutcliffe, K.M. (2003), «Das unerwartete Managen – Wie Unternehmen aus Extremsituationen lernen»
- Wyler, S. W. (1994), «Swiss Company Law In the European context», The New Swiss Company Law and the Euro-Council Directives, International Law Institute

Appendices

Appendix 1: Checklist for Implementing Enterprise Risk Management.. 182

Appendix 2: Example of a Risk Management Policy..... 184

Appendix 3: Example of Internal Regulations for Risk Committee 197

Appendix 4: Example of a Risk Identification Form..... 200

Appendix 5: Questionnaire for IT Risks 202

Appendix 6: Example of a Whistleblowing Policy Document..... 204

Appendix 7: ERM Self-Appraisal Questionnaire 208

Appendix 8: Guidance for FO2RDEC Analysis..... 212

Appendix 9: Job Description for Head of Risk Management/ CRO 215

Appendix 10: Example of an Individual Risk Assessment 217

Appendix 11: Insurance Check List for BoD..... 220

Appendix 12: Generic Collection of Master Risks..... 222

Appendix 13: Scenarios of the RESIST Methodology..... 223

Appendix 14: Examples of Anti-Corruption Controls..... 225

Appendix 15: Practical Guidance for the BoD on Uncontrollable Risks.. 229

Appendix 16: Elements of a Code of Conduct..... 233

Appendix 1: Checklist for Implementing Enterprise Risk Management

Phase 0: Evaluation Phase (6 months – 1 year)

Evaluation of existing

Business planning tools (e.g. BSC, EFQM)

Risk Management structure

Internal control policies and procedures

Quality control policies and procedures (e.g. ISO, TQM)

Risk Management tools (e.g. FMEA, HAZOP, Six Sigma)

Planning cycles (e.g. Strategy plans, Audit plans)

Reporting cycles

IT infrastructure (e.g. database, intranet)

Cultural environment

Phase I: Initiation Phase (6 months – 1 year)

Note: This phase is based on the findings from the evaluation phase

Setting of ERM objectives and goals

Definition of process

Definition of organisation

Development and communication of policies/ guidelines/ handbook

Nomination of person responsible for risks

Launch of pilot phase with risk identification at corporate level

Aggregation of all risks into master risk list (Risk Catalogue)

Assessment and prioritisation of risks through FMEA workshops

Information management through existing databases and tools

Phase II: Mitigation Phase (6 months – 1 year)

In-depth analysis of top risks (in CHF terms)

Mitigation measures based on risk-driver (root-cause) analysis

Implementation of mitigation measures

Planning for Business Continuity Management

Phase III: Controlling and Optimisation Phase (1 year)

Quarterly reporting and feedback

Feedback from internal/ external audit

Feedback from strategy control function	□
In-depth quantification and modelling of key long term risks	□
Extension of ERM process to divisions, SBUs and projects	□
External feedback and expertise	□
Train the trainers	□
Time-series analysis for existing top risks	□
Launch of web based Risk Management tool (for big companies)	□
Roll-out of Business Continuity Management project	□
Self-appraisal (annually)	□

Appendix 2: Example of a Risk Management Policy

VSOP LTD.

RISK POLICY

TABLE OF CONTENTS

1. PRINCIPLES OF RISK MANAGEMENT

- 1.1 Concept of the Risk Management
- 1.2 Purpose of the Risk Management
- 1.3 Strategy of the Risk Management
- 1.4 Annual Briefings
- 1.5 Risk Management Organisation
- 1.6 Roles and Responsibilities

2. RISK MANAGEMENT PROCESS

- 2.1 Process Phases
- 2.2 Overview of the Process

3. RISK MANAGEMENT GUIDELINES

- 3.1 Phase 0: Preparation
- 3.2 Phase 1: Risk Identification
- 3.3 Phase 2: Risk Assessment
- 3.4 Phase 3: Risk Measures
- 3.5 Phase 4: Risk Re-Mapping
- 3.6 Phase 5: Reporting

4. FINAL PROVISIONS

- 4.1 Entry into Force
- 4.2 Changes and Amendments

1. PRINCIPLES OF RISK MANAGEMENT

1.1 Concept of the Risk Management

The Risk Management (RM) of VSOP Ltd. is a task of the executive management and is monitored by the Board of Directors, defining an enterprise-wide strategic framework. It is designed to identify potential events that could have a substantial negative impact on the company. Its aim is to control risks and to ensure an adequate level of certainty in relation to the achievement of corporate goals. With the early identification of risks associated with the scope of the different departments, corporate risk preparedness and secureness should be increased. The RM of VSOP Ltd. is embedded in the existing management processes of the company and should not be a parallel organisation.

1.2 Purpose of the Risk Management

The main objective of the Risk Management is to provide the Board of Directors (BoD) and the executive management (EM) with a complete and continuously updated corporate risk overview. Based on this, the most important risks can be systematically processed according to their potential and be mitigated as far as possible. The main objectives include:

- Coordination of strategy, Risk Management and internal controls;
- Optimisation of decisions in response to risks;
- Improvement of the reliability of forecasts;
- Identification and control of enterprise-wide risks;
- Improvement of risk awareness throughout the company;
- Standardisation of procedures and the Risk Management language at the corporate level;
- Annual preparation of a top risks list which is respected and acted upon across all corresponding departments;
- Provision of adequate insurance coverage;
- Ensuring that the internal control system (ICS) is continuously implemented and optimised as far as possible.

1.3 Strategy of the Risk Management

Risk factors that may impact the ability of the company to reach its strategic objectives are detected and analysed. The Board and executive management of VSOP Ltd. are convinced that risks are always associated with opportunities. Calculated risk-taking is essential for the growth of our company. Each employee should be aware of the strategic direction of VSOP Ltd. and work to achieve these goals by taking reasonable steps, outlined below, to effectively manage risks and opportunities.

The strategy of VSOP Ltd. is based on the following vision:

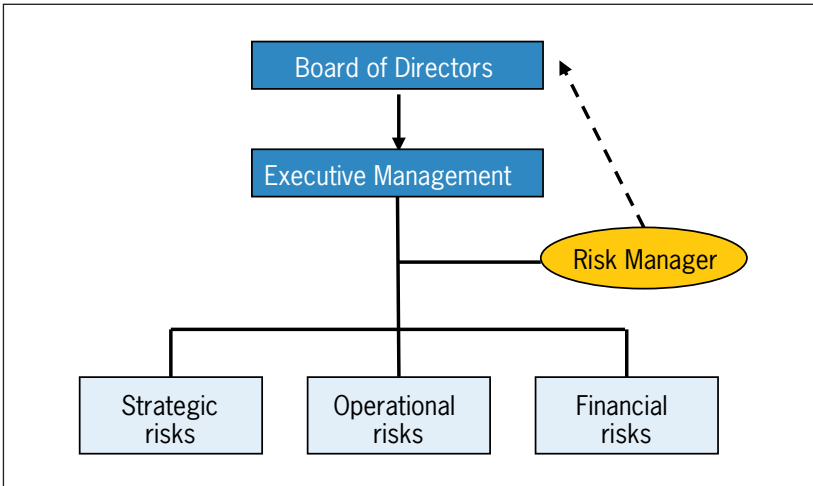
1. Take advantage of the growth opportunities in Switzerland through well-chosen market segments and service solutions;
2. Market leadership in Switzerland's aviation sector with the label Swiss Made;
3. Expansion of transportation services by offering state of the art transportation services in a global network.

1.4 Annual Briefings

The Board of Directors has to discuss the risk environment and the related risk exposure of VSOP Ltd. with the executive management at least once per annum. The findings are included in the risks and measures list. Ways to address and mitigate them are presented.

1.5 Risk Management Organisation

At VSOP Ltd., the Board of Directors has the overall responsibility for Risk Management. The board may seek advice from an advisory board, if such is established and needed. In line with the law, and based on company regulations, the Board delegates the implementation of Risk Management to the executive management (EM). The EM is assisted by the Risk Manager. He/ she acts on behalf of the EM and reports to them. In the case of urgent risks or if there is a concern that risks are not adequately perceived and / or handled, the Risk Manager can communicate directly with the Chairman of the Board.



1.6 Roles and Responsibilities

Board of Directors (BoD)

- Definition of the Risk Management organisation;
- Defining the Risk Management processes;
- Defining the Risk Management policy and the adoption of the policy;
- Ensuring the effective implementation of the Risk Management organisation, Risk Management policy and Risk Management processes;
- Taking overall responsibility for Risk Management

Executive Management (EM)

- Management of all risk factors within the strategic, operational and financial framework to mitigate and to reduce risks;
- Provide timely and accurate information about the risks that the company faces, as well as steps taken to ensure their effectiveness;
- Person in charge of implementation and coordination of the Risk Management;
- Coordination of information flow and documentation relating to the Risk Management;

- Conduct sampling to improve risk identification and evaluation and, if necessary, carry out a risk assessment and define appropriate risk-mitigating measures.

Risk Manager

- Preparation of annual risk analysis (as part of the annual SWOT analysis) for submission to EM and BoD;
- Preparation of the definition of risk-mitigating measures for submission to EM and BoD, as well as monitoring the implementation of the risk-mitigating measures;
- Quarterly reporting to the EM on the development of key risks and the level of risk-mitigating measures (risk radar as part of the quarterly reporting);
- Annual report on Risk Management to the BoD;
- Coordination of the Risk Management function with measures of the ICS;
- Ongoing identification, definition of proposed measures and reporting of significant changes in the risk environment;
- Preparation of the annual insurance overview;
- Ensuring that all employees are also questioned about new or worsened risks in connection with the annual staff performance review.

Risk Management is the responsibility of everyone in the company, including management and employees, and is therefore explicitly or implicitly part of the job description of every member of the company. In order to allow a proper application of that responsibility by all employees, the relevant Risk Management information will be published with access for all employees through the intranet.

2. RISK MANAGEMENT PROCESS

2.1 Process Phases

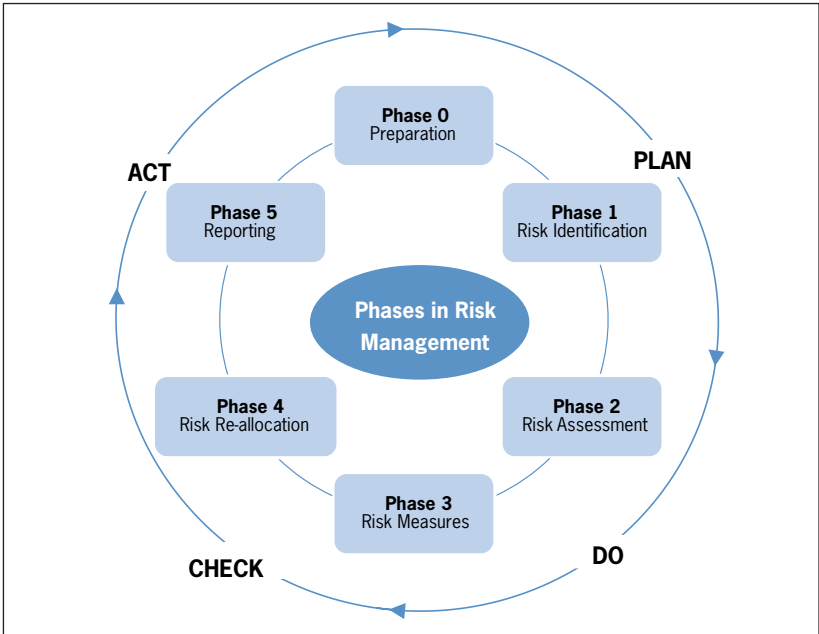
The overall process of risk identification, risk assessment, risk measures, risk re-allocation and reporting in the strategic environment should be carried out annually. In case of unforeseen and extraordinary events, these processes can occur more frequently.

Six Phases of the Risk Management Process:

- Phase 0: Preparation;
- Phase 1: Risk Identification;
- Phase 2: Risk Assessment;
- Phase 3: Risk Measures;
- Phase 4: Risk Re-allocation;
- Phase 5: Reporting.

2.2 Overview of the Process

The RM process is standardised across the whole company. The executive management undertakes all necessary efforts to raise the awareness of Risk Management amongst employees on every level.



3. RISK MANAGEMENT GUIDELINES

3.1 Phase 0: Preparation



The preparation phase is a long-term process and is not performed on an annual basis. It spans over a longer period and is modified and amended with changes in strategy, through extraordinary events or when new information becomes available. This phase includes the following tasks:

- Set up of the Risk Management organisation;
- Establishment of Risk Management processes;
- Issuance of the Risk Management policy;
- Definition of Risk Management guidelines.

Milestone 0: The definition, approval and implementation of the above tasks. Thereupon, the Risk Policy is adopted or revised by the Board of Directors.

3.2 Phase 1: Risk Identification

In this phase, all risks that confront VSOP Ltd. are identified. A risk can be described as an incident or event, triggered by an internal or external source, that may impact the implementation of a strategy or the achievement of objectives of VSOP Ltd. Risks can have either positive or negative effects; however, the focus of Risk Management activities at VSOP Ltd. is on negative events. At this stage, the executive management identifies and monitors all potential events, however low the probability of their occurrence may be. This is especially relevant if the potential impact on the achievement of important objectives is high.

In order to grasp all relevant risks, not just the BoD and EM members are interviewed by the Risk Manager. All employees of VSOP Ltd. have to be con-

sulted about possible risks, using a standardised questionnaire. Subsequently, this survey can be conducted in conjunction with the annual employee performance review.

Milestone 1: After the implementation of the Risk Management process all employees, as part of their annual employee performance review, are interviewed about possible new or worsened risks.

3.3 Phase 2: Risk Assessment

Step 1: Risk Consolidation and Classification

All identified risks are first consolidated by an interdisciplinary team composed of EM members and under the direction of the Risk Manager. Similar risks will be clustered and risks without a relevant damage potential will be removed from the classification. The risks are classified along the following three categories: strategic risks, operational risks and financial risks.

Strategic risks: This category covers risks that endanger the existence or continuation of the company, or which may cause the company to go into liquidation/insolvency. In general, these risks relate to the long-term success and viability of the company and include:

- Risks which arise from disasters or force majeure situations (e.g. service disruptions, uncertainties, service liabilities);
- Environmental risks: Strong competitors negatively affecting the business. Incorrect, untimely or unavailable information about competitors/rivals and their products could have an adverse effect on the business;
- Management risks: In addition to having an appropriate organisation, management style is one of the crucial preconditions for the success or failure of a company. Lack of leadership (unclear instructions, unclear responsibilities) may represent risks such as overdependence on leading executives;
- Risks related to stakeholders: Ensure that the company is focused on the needs and aspirations of all stakeholders, including shareholders and business partners, authorities, suppliers and society in general.

Operational risks: Operational risks are those risks that threaten strategic goals due to inappropriateness or lack of internal processes, people or systems. In general, these risks are short or medium-term risks and include the following:

- Process risks: Risks that relate to the process of customer value proposition in the company;
- Operational risks: Risks that arise in the daily operation such as insufficient resources, quality problems, illness, accidents, miscalculations, maintenance deficiencies;
- Infrastructure risks: Risks associated with the failure of important equipment for operations such as failure of the necessary IT infrastructure, etc.;
- People and cultural risks: Risks that arise as a result of years of corporate culture development and the people that live and work in this culture. There are several categories of such risks, and they may take the form of resources, know-how and skills, motivation, integrity, compensation, performance, relationship with trade unions and legal problems;
- Legal risks: Potential for losses arising from the uncertainty of future regulations or legal processes, such as outcomes of litigation, bankruptcy, etc.

Financial risks: Risks that have purely financial implications for the company (short or long term) fall in this category, for example:

- Market risks: The possibility of losses as a result of adverse changes in market prices and rates, including commodity prices, interest rates and exchange rates;
- Liquidity and credit risks: Liquidity risk describes a situation in which one party is not able to meet liabilities and debt obligations at a certain point in time. This may affect the management of liquid assets, hedging and financing;
- Taxes, regulations and accounting: Accounts are monitored closely; they may be affected substantially by the consequences from risks, e.g. fines or indemnifications due to lawsuits and legal measures;
- Capital structure: The company does not have sufficient/optimal capital, resulting in higher capital costs, lower profitability and a reduction in cash flow and liquidity.

Step 2: Risk Prioritisation

A workshop should be organised in order to prioritise risks in the master risks list. Members of executive management from selected departments and an external advisor all take part in this workshop. The idea is to encourage an open dialogue about risks.

All identified risks are analysed based on a risk priority number (RPN) which is based on two criteria and a weighting on a scale of 1-5. The criteria are defined as:

- The impact or severity of the event (effect of risk in financial terms);
- Probability of occurrence (frequency with which these risks occur).

The risk priority number (RPN) is obtained with the multiplication of the two risk factors. The lowest RPN is therefore 1 and the highest 25. Part of the risk assessment is also to determine whether a risk has a relevant lead time. This is considered as a surprise factor which is accounted for with the risk factor of -1. The prioritisation is made in the master risk list based on the determined RPN.

The master risk list should be treated as confidential by all employees. However, it may be required to present it to insurance brokers and insurance experts in connection with the annual insurance verification. A matrix to determine the RPN is shown below.

Disaster	>50M CHF	5	10	15	20	25
Critical	>5 <50M CHF	4	8	12	16	20
Moderate	>0,5 <5M CHF	3	6	9	12	15
Low	>0,05 <0,5M CHF	2	4	6	8	10
Insignificant	<0,05M CHF	1	2	3	4	5
Severity	Criteria	<1 per 100 years	>1 per 100 years <1 per 10 years	>1 per 10 years <1 per 1 year	>1 per year <1 per month	>1 per month
	Probability	Practically impossible	Unlikely	Possible	Occasional	Often

Zone 1	Risk is not acceptable, immediate measures for risk mitigation required
Zone 2	Tolerable risk, evaluate measures for risk mitigation
Zone 3	Acceptable risk, no measures required

Potential risks of more than 10 RPN, according to the risk assessment are the main risks (Top Risks) of VSOP Ltd. These risks have top priority for the following reasons:

- To direct the attention to the selected issues;
- To allocate the available resources (human capital or funds) efficiently;
- To assign risk owner(s) to each top risk.

Milestone 2: Identification, development and mapping of Top Risks.

3.4 Phase 3: Risk Measures

The measures for each of the key risks (Top Risks) are defined in an individual risk assessment including the following:

- The complete scenario of the risk occurrence;
- Drivers of the risk;
- The connection of this risk to other risks;
- Quantification of risk (intelligent estimate);
- Identification of the «need for action» and definition of the necessary risk-mitigating measures.

The detailed analysis must then be discussed with the executive management. Each risk is monitored by the Risk Manager along the following points:

- Clear and achievable goals and benchmarks;
- Detailed planning process, including clear deadlines, important milestones and cost-benefit analysis;

Definition of Key Performance Indicators (KPIs) or Standards;

- A clearly defined methodology;
- Clear allocation of resources.

Milestone 3: The measures for handling risks are defined, the action plan is prepared and persons responsible for each of the most important risks are appointed.

3.5 Phase 4: Risk Re-Mapping

The action plan for responding to a particular risk is set in a special project. The risk mapping should be updated in the second quarter of each year, along with trends in the risks in the top risks list and the effectiveness of responses to these risks. The re-mapping is important for the following reasons:

- To keep the development of risk scenarios in mind;
- The review of the effectiveness of measures for handling risks;
- To control the Risk Management process.

To ensure an accurate and complete understanding of all the potential risks, periodic surveys of all employees are conducted to obtain their risk assessment. Where possible, the risk re-mapping should be made by a multidisciplinary team.

Milestone 4: The individual risk assessments are continually processed by the respective risk owners in coordination with the Risk Manager.

3.6 Phase 5: Reporting

The reporting is prepared by the Risk Manager and the monitoring of the Risk Management process is documented as follows:

- Quarterly reporting to the EM concerning the major risks;
- Annual reporting of all risks according to the master risk list and the activities of the Risk Manager to the BoD;
- Annual update of all documents relating to the Risk Management.

In order to be able to update the Risk Management and reporting to the latest development standards, the Risk Manager should attend relevant training in consultation with the EM.

Milestone 5: Regular updates and reports on the follow-up process, the effectiveness of risk responses and proposals for the next cycle.

4. FINAL PROVISIONS

4.1 Entry into Force

With the resolution of the Board, this risk policy will be active with immediate effect and replace all previous provisions for Risk Management within VSOP Ltd..

4.2 Changes and Amendments

This risk policy has to be reviewed at least every four years and has to be amended if necessary.

Zürich, 1st of April 2015

Chairman of the Board of Directors:

Board secretary:

Appendix 3: Example of Internal Regulations for Risk Committee

VSOP Holding

Purpose

VSOP Holding has with immediate effect constituted a Risk Management Committee at the board level for the whole group of companies. The purpose that this committee will solve is as follows:

- Determine and assess all the strategic risks being faced by the group;
- To supervise the Risk Management process and have a complete overview;
- To confirm mitigating actions including insurances to keep the company's risk profile at an acceptable level;
- To report quarterly to the Board of Directors (BoD) and to make recommendations for further improvement of the company's Risk Management.

The committee will make spot-checks to manage the quality of Risk Management. It should be noted, however, that the creation of this committee does not relieve others from their Risk Management responsibilities. The ultimate responsibility for the success of the company and appropriate management of the risks, remains with the group CEO and the CEOs of various divisions.

Constitution

The committee shall be comprised of 3-5 members and deemed independent and objective. A minimum of three members (including the chairman) should be independent directors. The CEO and CFO are the ex-officio members of the committee. The members of the committee will be nominated by the Board of Directors (BoD) for a 1-year term with the possibility of extensions.

To guide the Risk Management process effectively, the committee shall be assisted by the Head of Risk Management. The position could be full-time, or present an additional responsibility, as deemed desirable by the Board of Directors (BoD).

Meetings

The Committee shall meet and report quarterly to the Board of Directors (BoD). In general, no quorum is required for meetings, but at least two-thirds of the committee must be present for decision-making. Proposals to the Board of Directors (BoD) and decisions must be taken by majority vote, with the casting vote of the chairman if necessary.

Meetings may be held by physical attendance or by telephone. Resolutions may be taken by letter, fax or email.

Minutes are to be taken at each committee meeting. These shall be taken by a secretary, who is not required to be a committee member. The minutes shall be signed by the committee's chairman and the secretary. The minutes shall be mailed to the members of the committee and the Board of Directors (BoD) within 14 days of the meeting.

Responsibilities

The Risk Management Committee shall have the following specific responsibilities:

- To create, manage and update a «Master Risk List» comprising the major risks and the corresponding mitigation actions to keep those risks at acceptable levels;
- To review proper management of the identified business and safety risks. This includes the necessary Risk Management process;
- To assist in the evaluation, instruction and supervision of the Head of Risk Management;
- To guarantee protection of data privacy;
- To supervise the conformity of all processes with legal requirements;
- To report quarterly to the Board of Directors (BoD) and to recommend measures for risk awareness, growth of positive Risk Management culture and information management.

The Audit Committee shall have the following responsibilities in relation to the Risk Management process:

- To survey the Risk Management process and provide an independent view to the Board of Directors (BoD);

- To review existing insurances and overview the correct payment of rates;
- To survey the mitigation of major risks, especially financial risks and IT risks;
- To survey the whistleblowing function.

Within the Risk Management process, the Nominations and Remunerations Committee shall assume the following responsibilities:

- Oversee recruiting and succession planning.

Authorised by the Board of Directors: Fantasyland, 01.02.2001

Chairman of the Board of Directors: Chairman of the Committee:

Michael Mann

Rick Montreux

Appendix 4: Example of a Risk Identification Form

Dear employees

Each Swiss publicly listed company is required by law to comment in the notes to financial statements on the implementation of management systems and, to that effect, to conduct regular risk assessments.

The term «Risk Management» means the permanent, systematic recording and analysis of all potential hazards and minimising all significant threats to the existence, operation and development of the company.

In order to avoid / mitigate risks in our company, the first step is to identify those. To do this we need your support. Surely you have seen during your daily work risks that could possibly bring our operations into serious trouble. Possible examples would be:

- Power outage during a long time;
- Loss of key customers;
- Failure of a critical machine;
- Foreign exchange risk for procurement.

Please reflect on what could constitute a risk for our firm in your view and indicate on the enclosed form by 30.06.2015 at least three of the biggest risks in your view

This survey serves as an important basis for management and administrative advice to better assess risk and to take appropriate and timely measures to minimise those. Thank you, therefore, already for your support and insights.

St. Gallen, April 1, 2015

For the Executive Board

Catherine Schmidt, CEO

Employee survey on Risk Management

I see the following key risks from the view point of my department / function

	Risk Description (Please provide detailed description to facilitate meaningful review)	Evaluation (By BoD / Executive Board)
1		
2		
3		
4		
5		

Name: Family Name:

Department: Function:

Appendix 5: Questionnaire for IT Risks

Identification and assessment of risks in the IT sector: Example Production Ltd.

Key Questions

Renewal Needs

- How long will the consisting hard- and software fulfil the company's requirements, on the one hand, and the customer's requirements, on the other hand?
- What financial consequences are generated for replacements?

Licence Monitoring

- Is only legally licensed, original software employed?
- Do enough licences for all users exist?

Support Monitoring

- Is future support warranted?
- Is it possible to provide alternatives quickly enough in case of the developing- and support-companies dropping out?

Data Recording

- What risks result from incorrect data entry?
- Are all actions taken to avoid incorrect data entry?

Data Filing

- Are the filed data stored long enough?
- Can filed data be utilised (read) in the far future?

Backup

- Are all relevant data saved?
- Are backups being made often enough?
- Are the filed data stored securely enough?
- Are checks of the filed data made periodically?

Data Security

- Are the data protected enough against external access?
- Are password checks reliable?
- Are passwords changed periodically?
- Is sufficient protection for data transfer to third parties ensured?

Apparatus Breakdown

- Are there alternatives in case of electrical power outage?
- Is the outage of single hardware components offset automatically by other hardware?
- Is the outage of the air-conditioning detected fast enough and eliminated through alternative actions?

IT-Knowhow

- Is all relevant information coherent with standard IT terms, especially hard- and software components, data filing and data security?
- Is complete adherence with written standards ensured?
- What know-how loss results from the outfall of an employee in the IT-division?

IT-Employee

- What damage can employees from the IT-division do if they transfer know-how to third parties?
- Is it ensured that an employee from the IT-division will not return to his workplace in case of redundancy?

IT-Contract Management

- Is a responsible person for IT-contract management nominated?
- Are contracts signed only with a clear limitation of costs?
- Is a control process for time limit and budget implemented?

IT-Project Management

- Is there an overview of IT-projects making explicit concrete priorities?
- Does every IT-project have defined responsibilities?
- Have the necessary financial and staff resources been identified for each IT-project and are they covered?
- Is adequate IT-project reporting established?
- Is there a system that assures that new IT-projects can be started only with the permission of the top IT responsible?

IT-Structure

- Is IT-structure sufficient for the far future and is there enough potential for further development?
- Are the databases used expandable and can they be migrated?
- What restrictions are given by the IT-structure regarding data flow and data utilisation?
- Are standard programs used or have individually programmed software solutions been implemented, making updates more difficult?

Appendix 6: Example of a Whistleblowing Policy Document

Policy Document: Whistleblowing at Example Production Ltd.

In keeping with the company policy of implementing the best practices in Corporate Governance, the Board of Directors (BoD) of Example Production Ltd. has initiated with immediate effect the following policy with regard to Whistleblowing. Whistleblowing in our organisation means the «disclosure of mismanagement, corruption, illegality, or some other wrongdoing, by a person or an employee in the organisation to those in authority».

Purpose

The purpose of this policy is to prevent fraud in accounting and auditing matters, and issues that could be detrimental to the reputation and sustainability of the company carried out with the malicious intent of either an employed individual or group. Furthermore, this document aims to enhance the confidence of employees to come forward and provide early warning in such situations.

Scope

Any event with a malicious intent to endanger the interest of the company and its stakeholders or for personal profiteering is worthy of being reported. Such events are listed below (Please note that this list is not exhaustive and Whistleblowers can categorise events as malicious subject to their own discretion. No action will be taken if the reported event does not fall under the defined category):

- Fraudulent and deceitful preparation of auditing, accounting and financial reports;
- Tampering with and/or destruction of company's auditing, accounting and financial records;
- Any observation with regard to conflicts of interest between company individuals and the company;
- Wrong and deceitful information to governmental and regulatory authorities;

- Intentional non-compliance with the internal controls and internal accounting of the company;
- Providing false information to investors, senior management, internal and external auditors;
- Non-compliance with the procedures laid out by the management that could result in major accidents, security breaches, product failures and loss of reputation;
- Organised stealing and theft from the production premises;
- Industrial sabotage;
- Leaking of sensitive and confidential information to competitors;
- Systematic racial and/or sexual harassment.

Whistleblowing Channels

The whistleblower has the following options to provide information:

- Personal meeting with the Chairman of the Ethics Committee/ Chairman of the Board/ Head of Risk Management. However, whistleblowers must also provide such information in writing for the records;
- Letter to the Chairman of the Ethics Committee/ Chairman of the Board/ Head of Risk Management;
- Email to the Chairman of the Ethics Committee/ Chairman of the Board/ Head of Risk Management; or
- By telephone to the following Hotline Number (007). All the calls on this number are automatically recorded and there is a provision to leave a message even during non-office hours. Recordings must be maintained and not deleted up to 5 years from the day they were registered.

The information generated from all these sources has to be shared with the General Counsel of the company immediately.

Company Doctrine

Example Production Ltd. is committed to provide the following with regards to its Whistleblowing policy:

- Whistleblowers can expect full protection (as provided under the law) with regard to their employment at the company and guarantee that they

are not subjected to any retaliation for their actions. On the other hand, misuse of the system for unethical and selfish purposes will also be dealt with appropriately in accordance with company laws and regulation;

- The identity of the whistleblower will be kept confidential to the maximum extent possible;
- The Ethics Committee will supervise the process including the review of complaints and necessary investigations. The committee could draw on internal and external expertise for appropriate management of the process according to their discretion and need. The external involvement is a must in the case of high level involvement and manipulation of financial reports and accounting and auditing statements. This assures independent and objective investigation. The external parties also are required to abide by the company laws and regulations following the highest level of integrity and confidentiality;
- The company will maintain and preserve all records generated for any future needs or reference;
- The company will share the information selectively with the various stakeholders keeping the strategic interests of the company and confidentiality requirements in focus.

Process

The Whistleblowing process at Example Production Ltd. Includes the following key steps:

- Receiving of complaint/ information;
- Notification to the Chairman of the Board of Directors (BoD) and Chairman of the Ethics Committee and General Counsel;
- Review by the Head of Risk Management and General Counsel;
- Feedback to the Chairman of the Ethics Committee regarding seriousness, extent, impacts, investigation requirements and investigation plans;
- Approval of the investigation plans by the board;
- Impartial and independent investigation;
- Findings of the investigations presented to Board Members, General Counsel and Head of Risk Management;
- Appropriate measures undertaken according to the results of the investi-

gation to be decided collectively by the Board of Directors (BoD);

- Bi-annual reporting by the Head of Risk Management to the Board Members and General Counsel on new complaints, those still under investigation, and those concluded in the last period.

Since the information involved could be of a highly sensitive and confidential nature only the following persons will have access to the reports and archived information.

- Board Members;
- General Counsel;
- Members of the investigative team;
- Head of Risk Management.

It is important that the confidentiality and anonymity of the complainant shall be safeguarded at all times during the entire process and after.

Mr. F. Müller
Chairman of the Board of
Directors (BoD)

Mr. Christoph Kaufmann
Chairman of the Ethics
Committee

Appendix 7: ERM Self-Appraisal Questionnaire

Please provide an appropriate response to the best of your knowledge using the scale below.
1 stands for 'strongly disagree' and 5 for 'strongly agree'

	Strongly Agree		Strongly disagree		
	1	2	3	4	5
Objectives					
The Risk Management objectives of our organisation are clearly defined	☐	☐	☐	☐	☐
The objectives are communicated to employees to provide effective direction to employees on risk assessment	☐	☐	☐	☐	☐
There is a clear understanding by management and others within the company of acceptable limits of risks set by the Board	☐	☐	☐	☐	☐
The board has a clear strategy for dealing with the significant risks	☐	☐	☐	☐	☐
There are comprehensive policies and guidelines for Risk Management in our company	☐	☐	☐	☐	☐
There is a comprehensive whistle blowing policy	☐	☐	☐	☐	☐
Structures					
I know the Risk Management organisation/ structure of my company	☐	☐	☐	☐	☐
The Risk Management organisation/ structure of my company is efficient	☐	☐	☐	☐	☐
Roles					
The roles of all the Risk Management participants are clearly defined	☐	☐	☐	☐	☐

The Risk Management workforce is highly competent	☐	☐	☐	☐	☐
The Board and senior management displays its commitment to Risk Management through its actions	☐	☐	☐	☐	☐
A large number of employees are involved for the efficient execution of Risk Management process	☐	☐	☐	☐	☐

Process

	1	2	3	4	5
Risks are linked to the strategic objectives of the company	☐	☐	☐	☐	☐
Strategic control function, internal auditing function and Risk Management function are integrated in our company	☐	☐	☐	☐	☐
Risk management process is linked closely to our existing management processes	☐	☐	☐	☐	☐
The Risk Management process at our company is systematic and standardised	☐	☐	☐	☐	☐
All significant risks are identified and assessed on an ongoing basis	☐	☐	☐	☐	☐
The present analysis (qualitative or quantitative) methodology is reliable	☐	☐	☐	☐	☐
There are proper follow-up procedures for the risks identified	☐	☐	☐	☐	☐
There is clear allocation of resources for managing top risks	☐	☐	☐	☐	☐

Reporting

	1	2	3	4	5
The Board and top management receive regularly the standardised and systematic risk reports	☐	☐	☐	☐	☐

The information included in the risk report is reliable	☐	☐	☐	☐	☐
---	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

The company has access to historical information about risks	☐	☐	☐	☐	☐
--	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

Communication

	1	2	3	4	5
Shareholders have an accurate picture of company's risk profile	☐	☐	☐	☐	☐

I know top risks of my company	☐	☐	☐	☐	☐
--------------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

I am aware of the major risk mitigation actions undertaken	☐	☐	☐	☐	☐
--	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

I am clearly informed as to what is required of me with regard to Risk Management within the organisation	☐	☐	☐	☐	☐
---	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

I know the strategic objectives of the company	☐	☐	☐	☐	☐
--	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

I know how the strategic objectives of our company are linked to the top risks	☐	☐	☐	☐	☐
--	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

Culture

	1	2	3	4	5
Company has a reward structure for supporting and achieving Risk Management objectives	☐	☐	☐	☐	☐

Risk management training is available	☐	☐	☐	☐	☐
---------------------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

My opinion is respected and given due importance in Risk Management decisions	☐	☐	☐	☐	☐
---	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

I can pass the risk information to the top management and Board without following hierarchical structures	☐	☐	☐	☐	☐
---	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

I have no fear or reservations in freely passing the risk related information to the Board and top management	☐	☐	☐	☐	☐
---	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

I clearly observe the benefit and importance of Risk Management in our company	☐	☐	☐	☐	☐
I know of instances when Risk Management has saved/ added value for the company	☐	☐	☐	☐	☐
Risk management support staff is easily accessible	☐	☐	☐	☐	☐

Tools

	1	2	3	4	5
We have Risk Management tools	☐	☐	☐	☐	☐
We have an IT Tool for supporting the Risk Management process at the company	☐	☐	☐	☐	☐
The present IT Tool adequately supports the Risk Management process	☐	☐	☐	☐	☐

Business Continuity Management

	1	2	3	4	5
I am aware of risks/ catastrophes which can threaten the existence of the company	☐	☐	☐	☐	☐
We have a business continuity plan in place	☐	☐	☐	☐	☐
All the employees know their roles in case of a catastrophe	☐	☐	☐	☐	☐
We have back up servers to protect data	☐	☐	☐	☐	☐
We have regular crisis management drills	☐	☐	☐	☐	☐
We have diversified our assets geographically so that catastrophes do not threaten our existence	☐	☐	☐	☐	☐

Remarks

- This questionnaire should be circulated throughout the organisation once every year
- The company should endeavour to get as many respondents as practically possible from different hierarchical levels and functions
- An average score of less than 3 signifies insufficient Risk Management in the company. The sections with low scores signify the area of weakness that must be investigated and improved

Appendix 8: Guidance for FO²RDEC Analysis

If time constraints leave enough space for it, the FO²RDEC analysis constitutes a structured model process of finding sustainable solutions to be applied for important decisions. This model is not suitable though for taking immediate decisions e.g. in the operations room of a nuclear plant, in a cockpit or on the navigation bridge of an aircraft carrier, as the model requires different processes and preparations to be applied. The FO²RDEC analysis concerns both strategic and important operative or technical decisions with a potential impact on the specific project, a plant or a company as a whole.

The acronym FO²RDEC stands for the following structure elements in the process of decision-finding:¹⁶⁵

- **Facts** analysing the initial situation, project, plant condition
- **Objectives** intended condition / target
- **Options** suggestions and options
- **Risks** advantages and downsides of potential solutions
- **Decision** selecting the best, i.e. optimal solution
- **Execution** translating the decision into practice
- **Check** effectiveness control / lessons learnt

Functions

As a rule, the following functions need to be represented when performing a FO²RDEC analysis:

Team leader: A person with a decision-making authority within the project and/or organisation.

Moderator: The team leader decides whether to appoint a moderator (this can be advisable whenever the team leader is to become an active participant in the decision-finding discussion). If no moderator is appointed, the function is held by the team leader.

¹⁶⁵ Cf. Hörmann (1994); Hörmann, H.-J. (1995: 17-23)

Secretary: Is responsible for minute-taking and appropriate documentation of relevant facts during the decision-finding process and in the final proceedings.

Team members: The team should possess all the decision-relevant professional expertise. For this purpose, it may become necessary to adapt the team composition during the decision-finding process.

Although situations of this kind occur quite frequently at different committees of a board, and the board itself often finds itself in similar circumstances, only rarely do decision-making bodies make use of structured decision-making models.

Progression of the FO²RDEC analysis

At the beginning of the process the team leader explains the goals of the committee, organises an appropriate basis for work (e.g. appointment of a moderator, providing necessary information, documents and/or contacts to external experts) and sets the timeline.

F: At this first stage all known facts supported by findings are gathered. At this point, it is important to avoid any speculation. The moderator asks every team member to present the facts and their personal assessment of the task at hand.

O: The intended status, goal or outcome are defined at this stage and adopted by all team members. The moderator highlights the points in common and the differences in the assessment and ensures that every team member has presented his or her input. The moderator then summarises the problem and facilitates an appropriate presentation of the goals and priorities.

O: Options and possible actions (not only the obvious ones) are gathered at this stage, whereby any evaluation should be avoided. The moderator asks all team members to present their solutions, makes a summary and ensures that every team member was given a possibility to provide his or her feedback.

- R: Risks, advantages and disadvantages of individual options are analysed in a systematic way based on a set of criteria, if possible. The criteria used for this purpose should make it possible to assess the measure of the achievement.
- D: The team leader takes a decision, justifies it and asks the team members to present their doubts if any.
- E: The team leader determines the functions, timeline and possible break-points for the implementation.
- C: The time of review of the intended outcome is defined at this stage. During the review, the measure of achievement is assessed according to the criteria (as per «R»). As a result, lessons learnt are formulated and communicated to the relevant decision-makers within the organisation.

In the case of non-achievement it is necessary to carry out a further FO²R-DEC analysis.

Decision-making on the basis of FO²RDEC model is, clearly, no silver bullet against possible errors yet it allows to considerably reduce the risk of errors whilst providing an inclusive platform for all relevant experts – thus preventing the appearance of a culture of autonomous decisions and non-consulting.

Appendix 9: Job Description for Head of Risk Management/CRO

General Information

Job Title	Head of Risk Management/ Chief Risk Officer (CRO)
Sponsored by	Executive Board
Supervisor	CEO
Start date	1. April 2015
Job percent	30 Percent
Deputy	CFO
Additional functional responsibility	Head of Quality
Signing Authority	None
Authorisations	Right to inspect all business documents, right to obtain information about all employees, report directly to the Board President

Responsibilities

- Monitoring and optimisation of the Risk Management process;
- Ongoing mitigation of the main risks of sample production AG;
- Ensure adequate insurance protection.

Job requirements

- Social and inter-personal skills;
 - ▷ Independent, accurate and structured way of working;
 - ▷ Flexible and durable, to solve problems;
 - ▷ Creative and open to new ideas and changes;
 - ▷ Loyal and discreet;
 - ▷ Planning and organisational skills.
- Expertise;
 - ▷ Basic Training in Risk Management (preferably supported by a university degree or equivalent and minimum 5 years of experience);
 - ▷ Interdisciplinary understanding;
 - ▷ Lateral thinker;
 - ▷ Organisational and project management skills;

- ▷ Willing to undergo continuous training in Risk Management.

Core activities

- Risk Analysis;
 - ▷ Preparation of annual risk analysis (as part of the annual SWOT analysis) for submission to Executive Board and BoD;
 - ▷ Ongoing identification of risks and preparing proposal for mitigating measures and reporting of significant changes in the risk environment;
 - ▷ Ensure that all employees are also evaluated on their Risk Management performance in their annual performance analyses, including identifying, monitoring and management of risks related to their area or responsibility;
- Establish appropriate reports for Executive Board and BoD;
 - ▷ Quarterly reporting to the Executive Board on the development of key risks and the status of risk-mitigating measures (including establishing risk radar as part of quarterly reporting);
 - ▷ Annual report on Risk Management to the Board.
- Coordination of the Risk Management function aligned with its measures;
- Preparation of annual insurance overview;
- Advising the Executive Board in Risk Management related issues.

Special Tasks

On advice of CEO, person in charge for RM can be assigned additional functions, particularly in relation to specific projects.

Appendix 10: Example of an Individual Risk Assessment

RISK MANAGEMENT SAMPLE COMPANY

Individual Risk Assessment

Risk No. 9 Exchange Rate Development

Introduction

As part of the Risk Management of the sample company, all potential sources of risk in relation to existence, operation and development of the company are systematically recorded and analysed. The recognised and relevant risks are assessed according to standard criteria regarding financial scope, frequency of occurrence and severity. The resulting risks are then entered into a Master Risk List according to their priority and risk factor. This is the basis for the individual risk assessment in which the significant risks are presented and mitigation measures are proposed to reduce the level of risk.

Starting point: No. 9 Exchange rate risk developments

- Changes in exchange rates might not only affect income and costs, but also the assets and liabilities of the sample company extremely unfavourably. The sample company invoices in the following currencies: CHF, EUR, USD and YEN. As an exporter, the strength of CHF in recent years is, in the view of the sample company, no advantage.
- For several years, the sample company has assured the currencies CHF, EUR and USD, but not YEN, with financial instruments against downward trends, with the aim of planning security. The corresponding operating margin is described in the mandatory foreign currency directive of October 3rd in 2013.
- For a natural hedging, the possibilities for the sample company are low, e.g. no production facility in the USD or YEN-area, limited ability to pay suppliers and employees in EUR.

Risk No. 9 Exchange rate development

Risk owner	CFO Karl Muster
Probability	Development (gradual) ☐ ☐ ☒ Event (unexpected)
Risk area	Finance
Hazard	Market prices (Master Risk List item 6.2)
Cause of the risk	Negative exchange rate development Declining sales prices for deliveries abroad (export) Decline in international business because foreign competitors can offer more price-favourable products (arbitrage) Lack of currency risk hedging Rising inflation

Goals	Procedure/ Action item
☐ Avoid risk ☒ Mitigate risk ☐ Accept risk	Early warning indicators Exchange rates of banks, etc.
Reduction of frequency	Implementation of the foreign currency directive
Reduction of severity	Ongoing completion of foreign currency exchange contracts in accordance with foreign currency guidelines Limit holdings of unhedged currencies Prevent opportunities for speculation with currencies, financial instruments, etc. No additional building-up of exchange rate risks with medium and long-term investment in securities

Measure	Responsible	Deadline	Status
Completed measures			
Creating a foreign currency policy	John Doe	30.06.2010	Completed
Check if the YEN currency should be hedged	John Doe	30.09.2011	Completed

Measure	Responsible	Deadline	Status
Pending actions			
Use of hedging instruments at UBS in Zurich	John Doe	31.12.2014	In progress
Regular assessment of the currency positions relative to price limits and stocks (a currency may not exceed a certain amount)	John Doe	31.12.2014	In progress
Waiver of financial instruments and systems that include additional currency risks	John Doe	30.06.2014	In Progress
Annual review of pricing arrangements with our subsidiaries regarding currency surcharge or markdown	John Doe	31.12.2014	In Progress
Check if a group-wide cash pooling could be useful and practical	John Doe	31.03.2014	In Progress

Appendix 11: Insurance Check List for BoD

1. Does the range of insurance policies of the company cover all non-life and all personal insurances?

→ List details for each insurance in a table

Insurance Policy	Insurer	Sum Assured	Insurance Term	Comments
A				
B				

NON-LIFE

Property Insurance

- Damage by Fire / Water / Theft / Damage of Glass
- Business Interruption – Premises / Contents
- General Damages
- Insurance against Terror

Technical Insurance

- IT Equipment / Infrastructure
- Record Carrier Repair / Data Recovery
- Machinery and Equipment
- Business Interruption of Machinery
- Construction Insurance
- Installation / Commissioning

Transportation Insurance

- Goods-in-Transit Insurance
- Exhibitions / Fairs
- Business Interruption – Transportation
- Freight / Carrier Liability
- Warehousing
- Hull / Collision Insurance
- Valuables Insurance
- Luggage Insurance

Motor Insurance

- Liability Insurance
- Hull / Hull Partial Damage
- Accident Insurance
- Bonus Protection
- Gross Negligence
- Passenger Insurance
- Water Vehicles

Insurance of Assets

- Interruption of Business
- Merchandising / Packaging
- Product Recall
- Loading and Unloading
- Defence and Recovery
- Environmental Pollution Policy
- Directors' and Officers' Liability Insurance
- Building Liabilities Insurance

Other Insurances

- Protection of Industrial Property
- Defence and Recovery for Motor Vehicles
- Defence and Recovery for Contracts
- Sureties Insurance
- Credits / Encashment
- Guarantees Insurance
- Cancellation Charges

PERSONAL

Occupational Pension Funds

- Pension Fund basic
- Pension Fund supplement
- Pension Fund Counter Guarantees

Accident Insurance

- Accident at Work
- Medical Treatment
- Disability Pensions
- Special Risks
- Customer and Visitors Accident
- Collective Accident
- Single Accident

Sickness

- Daily Benefits Payments
- Loss of Earnings Insurance for Maternity
- Survivor's Pensions

Special Risks

- Life Insurance
- Guests/ Interns
- Travel Insurance
- Deficiency of Key Personnel
- Kidnapping and Extortion
- Discrimination
- Product Protection
- Data Abuse

2. **Are the Risks on the Master Risk List covered by appropriate insurances as far as possible?**
→ YES/NO (define measures)
3. **Do the respective insurances offer enough protection against the risks or recovery for the event that they would materialise?**
→ YES/NO (define measures)
4. **Are the terms of the policies long enough compared to the risks involved?**
→ YES/NO (define measures)
5. **Is the company double-insured with regard to any risk topics?**
→ YES/NO (define measures)
6. **If risks/risk measures are defined legally, do the corresponding insurances live up to the standards the law stipulates?**
→ YES/NO (define measures)
7. **Does the company have an insurance assessment from an insurance broker?**
→ YES/NO (define measures)
8. **Is there a confirmation by the insurance broker, especially with respect to the General Terms and Conditions (GTC)?**
→ YES/NO (define measures)
9. **Are the retrocessions and commissions related to the insurance contracts – especially the recent ones) transparent (e.g. amounts, recipients, extension conditions)?**
→ YES/NO (define measures)

Appendix 12: Generic Collection of Master Risks

Fantasy Engineering AG

Markets

1. Change of macroeconomic situation (of main markets)
2. Market volume development
3. Competitors
4. Political environment

Clients

5. Customer portfolio
6. Customer losses
7. Satisfaction level of customers

Products / Services

8. Product / service portfolio
9. Product / service life cycle
10. Product / service quality

Safety and Security

11. Technical Safety
12. Health, hygiene and safety
13. Security

Core processes

14. Product innovation and development (R&D)
15. Supply and logistics
16. Production (incl. service processes)
17. Sales, price and distribution
18. After sales service
19. Trade mark and reputation

Corporate Governance

20. Planning
21. Organisational structure
22. Communication
23. Reporting
24. Projects
25. Investments incl. acquisition
26. Alliances and co-operations
27. Risk Management

Human Resources

28. Resources, know-how and skills
29. Integrity and reliability of personnel
30. Motivation
31. Performance compensation
32. Trade union relations

Commitments

33. Contract liabilities
34. Claims and collaterals
35. Product liabilities
36. Ethical liabilities
37. Moral obligations

Finance

38. Cash flow
39. Access to funding / interest rate
40. Payment system
41. Foreign exchange risk
42. Accounting reliability

Assets

43. Failures due to natural disasters
44. Fixed Assets (including valuation)
45. Inventory (including valuation)

Information Technology

46. Integrity
47. Availability

Laws/Regulations

48. Compliance with laws
49. Compliance with regulations
50. Tax laws (including optimisation)

Appendix 13: Scenarios of the RESIST Methodology

1	In a bidding round, the terms of reference (including technical specifications) are biased to favour one supplier or to exclude potential competitors
2	Intermediary offers company to win bidding upon payment of loser's fee during pre-bidding or bidding stage
3	Bribe solicitation for confidential information during pre-bidding or bidding stage
4	«Kickback» scenario: Your sales representative is offered hidden compensation by the customer or by an intermediary
5	A host country may impose or imposes a partnership with a designated local company that may present high corruption risks
6	Client demands a last-minute «closure fee» to close a deal that is now too late to lose
7	A company complaining about an unfair procurement process is threatened with a spurious criminal prosecution that will lead to a heavy fine
8	A local government agency demands a fee for technical approval of equipment
9	Newly-hired employees cannot obtain work permits unless an employment surcharge is paid
10	A local police officer requests a payment to allow an expatriate worker to cross an internal border within a country
11	An employee of the state electricity company demands cash for connection to the grid
12	Long-awaited essential equipment is stuck in customs for clearance and only the payment of a «special» fee can secure its prompt release
13	Perishable goods are held up in customs and will only be released if a cash payment is made
14	A tax inspector asks for a «kickback» in exchange for granting a discharge or accepting a settlement in a tax dispute
15	A union leader demands payment to an employee welfare fund before allowing his/her members to unload a ship
16	A client asks your company to arrange and pay for a check-up at a prestigious hospital while on a visit to your home office

17	A government official requests free product samples for private use
18	A government representative requests sponsorship for an activity linked to the private interests of high-level government officials
19	A financial services intermediary demands incentives over and above the regulated commissions and fees for referral of clients to financial product providers
20	A supplier offers a bribe to a contract manager to overlook «out of spec» or inferior goods or services
21	A customer representative demands a fee that was not previously agreed as a condition to a contract change
22	For a fee, a «businessperson» offers to help reinstate client progress payments that were stopped for no apparent reason

(Source: <http://www.iccwbo.org/products-and-services/fighting-commercial-crime/resist/>)

Appendix 14: Examples of Anti-Corruption Controls¹⁶⁶

Typical general entity-level anti-corruption controls

- A formal anti-corruption compliance programme;
- An Anti-Corruption or Compliance Committee mandated to review or receive updates on all high-risk transactions;
- Written standards (i.e., the code of conduct and anti-corruption and other related policies);
- Anti-corruption training and communication for employees;
- Tone from the top and the middle;
- Employee background checks;
- Whistleblower system;
- Gift, entertainment, and hospitality request approval and tracking;
- Conflict of interest certification/disclosure process;
- Third-party contract provision on compliance;
- A competitive bidding/selection process including RFP dissemination to prospective vendors and proposal review;
- Risk tier classification system for third parties;
- Third party due diligence (in line with the designated risk tier);
- Multiple levels of vendor contract approval or internal sign-off (e.g., requiring approval from procurement, the legal and compliance functions, and local management);
- Accounting controls on vendor invoice review, approval, and payment;
- A process for travel and expense report review, approval, and reimbursement;
- An employee culture of ethics and knowledge assessment;
- Exit interviews;
- Mandatory anti-corruption audits on regularly recurring basis;
- Mandatory rotation of key management level personnel in high risk locations.

¹⁶⁶ From: A Guide for Anti-Corruption Risk Assessment (<https://www.unglobalcompact.org/resources/411>)

Scheme-specific controls

(Including some that may be a scheme-specific version of an entity-level control)

A scheme using consultants/fixers as bribery conduits may include the following mitigating controls and processes:

- A process for documenting a business need for hiring a consultant;
- Consultant due diligence/screening with specific aspects such as background check, screening against politically exposed persons («PEP») lists, a references and credentials check, prior engagements, reputation and a sample work product review (depending on the risk tier);
- Consultant certification of compliance (initial and at periodic intervals, e.g., annually) such as an anti-corruption policy acknowledgement and certification, a vendor code of conduct;
- Anti-corruption training and communication activities targeted to the procurement personnel involved as well as to the consultant's hiring/ongoing management and to the consultant him/herself;
- Periodic consultant performance evaluations, actual work product review;
- Consultant fee/invoice analyses (does the invoice have an adequate level of detail, is the fee reasonable, how does it compare with other similar vendors, is it commensurate with the work product, is there a correlation between a consultant invoice and a particular government action that benefited the enterprise).

A scheme involving commercial enterprise sales reps providing potentially inappropriate gifts, hospitality, and entertainment to prospects or customers may include the following:

- Periodic gift and entertainment training and communication targeted to sales personnel and their managers;
- Communication to customers about the enterprise's gift, hospitality and entertainment policy;
- Tone from the middle: communication to sales personnel from supervisors or market leadership;
- Periodic (e.g. annual) anti-corruption policy acknowledgement or certification among sales personnel and supervisors;
- Mandatory use of the enterprise's credit cards for any third party meals or

other entertainment by sales personnel;

- Sales representative rotation;
- Customer survey/interviews;
- Hotline availability for customer personnel.

Preventative anti-corruption controls

- Having a formal anti-corruption programme in place with a defined structure, ownership, reporting lines and planned activities and periodic measurement for effectiveness;
- Written standards (code, anti-corruption policies);
- Anti-corruption training and communication, including a resource library;
- Tone from the top and the middle: visible senior and mid-level managements setting the expectations;
- A risk classification system for third parties, corporate locations and business activities (i.e. a tiered system whereby higher risk parties would be subjected to a more robust due diligence and oversight than lower risk parties);
- Due care and due diligence, including personnel background checks, third party initial due diligence, policy certification/acknowledgement;
- Gift, hospitality, and entertainment advance approval;
- Segregation of duties;
- Contract provisions on compliance with the law in general and anti-bribery specifically;
- Incentives for proper conduct, ethics awards and (to some extent) performance evaluations with specific ethics and compliance provisions.

For many schemes, preventative controls could be augmented by detective controls, for the purpose of early detection of misconduct (both intentional and unintentional).

Detective anti-corruption controls

- Gift, hospitality and entertainment tracking (after the fact);
- Expense report audit;

- Periodic third party monitoring (e.g., performance assessment, re-certification);
- Whistleblower system, investigation process and case management;
- Exit interviews;
- Corporate audit, transaction audit, third party audit;
- Employee culture of ethics and compliance assessment, particularly if it includes questions
 - about pressure to commit misconduct, actual policy violation;
- Customer, vendor, or third party survey or interview.

Appendix 15: Practical Guidance for the BoD on Uncontrollable Risks

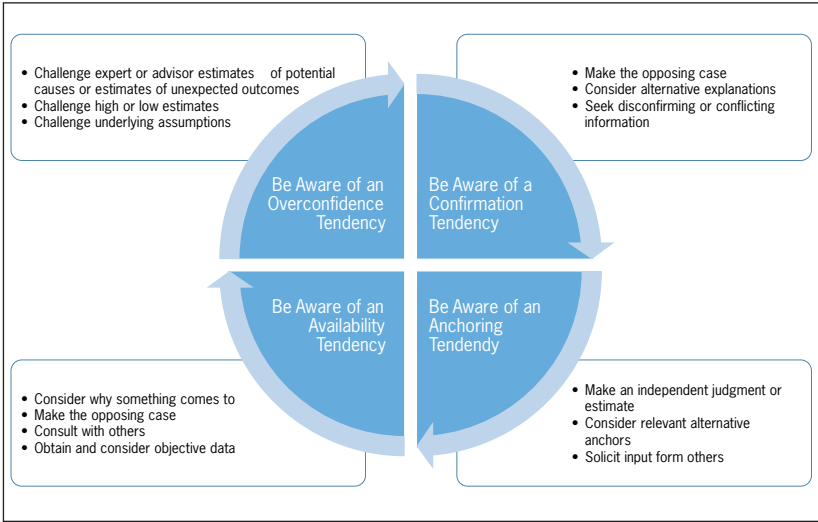
If a Board of Directors (BoD) accepts that underlying relationship between connectivity, complexity and uncertainty in the context of uncontrollable risks, then what steps should it take given its supervisory responsibilities?

A Board of Directors should consider three «lines of defence» in response to the challenge of uncontrollable risks:

1st line of defence is Board Diversity

The first inquiry the BoD should make is whether there is a «diversity of thinking» within its own membership to mitigate against judgment biases. Perceptions of risk and control can vary not only based on academic training or professional experience but also on gender, geographic and generational differences (see figure below).

Mitigating Biases in Judgment



Source: Adapted from COSO, Exhibit 3 (2012: 16).

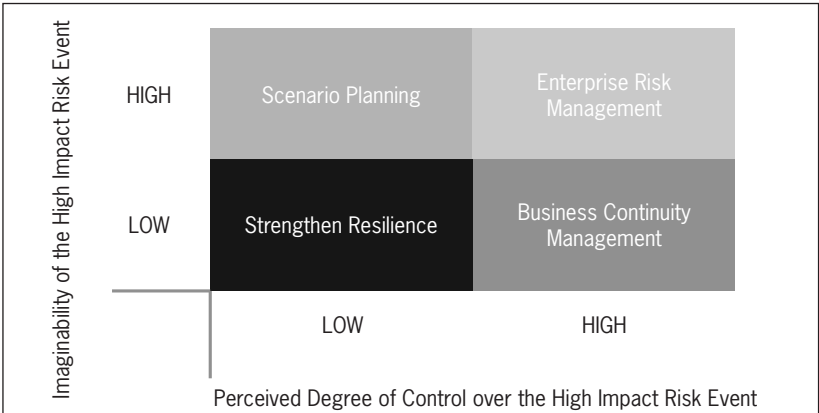
2nd line of defence is Risk Mapping

The first action the BoD should consider is to review the company’s master risk list and their distribution across the company’s risk map (typically the x-axis measures the probability of occurrence and the y-axis measure impact). The BoD should then consider the following four lines of inquiry (checklist) during the board’s review:

- Q1: How are these risks possibly related to each other and are there intersecting vulnerabilities?
- Q2: If there are such connections, are there cascading consequences to consider?
- Q3: What is missing from the risk map? And why?
- Q4: Are they not listed because they are not plausible – i.e. unimaginable in the current context?
- Q5: Are they not listed because they are exogenous or systemic and beyond the company’s control?

If clear examples are provided in response to Q4 and Q5, the BoD should consider the framework below to identify the appropriate means to address that particular example.

Uncontrollable Risks: A Response Framework for Boards

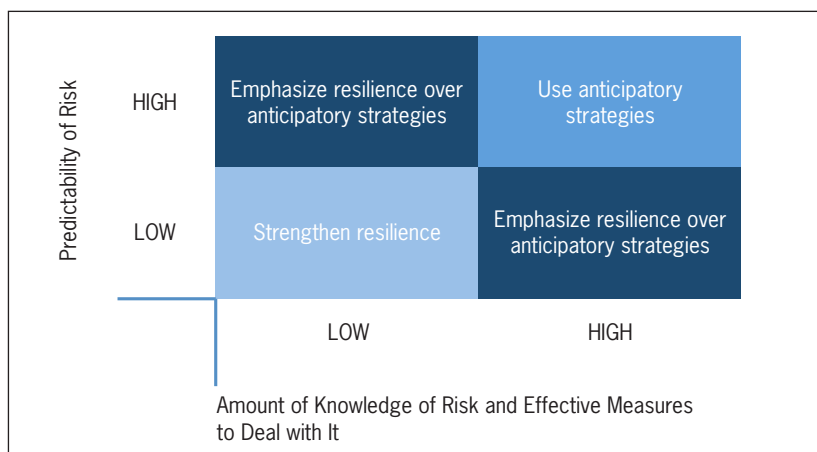


Source: Author

3rd line of defence is Organisational Resilience

In addition to supervision of the company's Risk Management, the BoD should on an annual basis review their company's organisational resilience if a Black Swan Event were to occur. The first step of the review should be to identify those risks where the ability to predict it is very low and the amount of knowledge about the risk (including mitigation measures) is also very low – for those identified the company should consider measures to strengthen organisational resilience rather than attempting to predict or prevent the occurrence of the risk event (see figure below).

Board Framework on Resilience



Source: Adapted from WEF, Figure 21 (2013: 37).

In attempting to assess the company's organisational resilience, the BoD should determine if the company is a hierarchical or networked organisation by evaluating the following criteria (see table below):

Assessing Organisational Resilience

Attributes of the Organisation	Hierarchical Attributes	Networked Attributes
Leadership Style	Centralised	Distributed
Interdependence of Business Units	Tightly Coupled	Loosely Coupled
Workforce Location	Concentrated	Dispersed
Talent Recruitment	Specialists	Cross-trained Generalists
Control & Direction	Policy and procedure driven	Guided by simple yet flexible rules

Sources: Adapted from WEF, Figure 25 (2012: 33).

Based on their observation, the BoD should determine if the company is more hierarchical or networked. A networked organisation is presumed to be more resilient (i.e. more resistant to the impacts of a sustained crisis).

Appendix 16: Elements of a Code of Conduct

Codes of business conduct come in many shapes and forms. Where US companies often rely on longer, rule-based codes with detailed descriptions and examples, European companies usually prefer shorter, principle-based codes of conduct offering guidance on a high-level only. There is a clear trend towards uniformity in codes of conduct. Although there are variations between industries (e.g. Pharma and Finance), most codes nowadays cover the following topics:

1. Introduction
 - ▷ CEO / Chairman message
 - ▷ Values / Principles
 - ▷ Scope of code (stakeholders)
2. Compliance with conventions, laws and regulations, for instance:
 - ▷ Anti-trust / Anti-competition
 - ▷ Anti-bribery / Corruption
 - ▷ Anti-money Laundering / Terrorist financing
3. Protection of company assets
4. Improper payments, Gifts and Entertainment
 - ▷ Bribes and Facilitation payments
 - ▷ Giving / accepting Gifts and Entertainment
 - ▷ Political / Charitable contributions and sponsoring
5. Conflicts of interest, e.g.
 - ▷ Insider dealing
 - ▷ Board positions
 - ▷ Political activities
 - ▷ Family relationships
6. Workplace ethics, for instance
 - ▷ Discrimination
 - ▷ Harassment
 - ▷ Health, Safety, Environment
7. Accurate reporting
8. Confidential information
 - ▷ Client, Market information
 - ▷ Employee data
 - ▷ Intellectual property
9. Reporting misconduct
 - ▷ Hotline / Ombudsfunction
 - ▷ Anonymous reporting / Retaliation
 - ▷ Follow-up on reports
10. Glossary / References
 - ▷ Definitions
 - ▷ Policy documents
 - ▷ External sources
11. Contact details

Editors



Dr.oec. HSG Vinay Kalia

Vinay Kalia works as an Operational Risk Manager for UBS, within Compliance and Operational Risk Control. Prior to this position he was employed at the international Auditing firm KPMG Limited, Switzerland, as manager at Risk and Sustainability Advisory Services. During his PhD, while assisting Prof. Roman Boutellier at the Swiss Federal Institute of Technology, Zurich (ETHZ), benchmarked best in the class Risk Managed Companies, by advising some companies within Switzerland. He is a portfolio partner at the International Center for Corporate Governance University of St. Gallen (www.icfcg.org) with expertise in Enterprise Risk Management. Vinay has attained an MBA from the Nanyang Business School, Singapore and is currently the president of Nanyang Technological University Alumni, Europe Chapter. From the earlier part of his life and career, he brings a broad set of experience such as knowhow in Hospitality and Tourism industry in Asia including India and Singapore.



Prof. Dr.iur. Roland Müller

Roland Müller is Chairman and Member of the Board of Directors of several Swiss Companies with keen interest in establishing best practice Risk Management values. His background includes law studies at the universities of Geneva and Zurich and he has attained Master of Law and PhD from the University of Zurich. Since 1985 he has been a lawyer and notary public. Since 1992, he is senior partner in the law firm ME Advocat Rechtsanwälte, Staad. From 2000 to 2006 he was Chairman of the Risk Management Committee at SR Technics in Zurich. In 2005, he completed his habilitation at the University of St. Gallen and was appointed Adjunct Professor at the University of St. Gallen for Private Law, Commercial Law and Air Law. In 2014, the University of Berne awarded him the title of Professor.