

Vinay Kalia / Roland Müller

Risk Management at Board Level  
A Practical Guide for Board Members

**■ Haupt**

Dr. oec. HSG Vinay Kalia

Vinay Kalia is currently a Senior Associate in the International Auditing firm KPMG Fides Peat, Switzerland and portfolio partner at the IFPM, Center for Corporate Governance, University of St. Gallen ([www.ccg.ifpm.unisg.ch](http://www.ccg.ifpm.unisg.ch)) in Enterprise Risk Management. He has dedicated last 4½ years on researching risk management at the Board and management level in Swiss and international organizations while closely collaborating with the leading companies in Switzerland and Europe. Prior to this, Vinay has attained an MBA from the Nanyang Business School, Singapore and has diverse experience in Hospitality and Tourism industry in Asia including India and Singapore.

PD Dr.iur. Roland Müller

Roland Müller is Chairman and Member of the Board of Directors of several Swiss Companies with a 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 Müller Eckstein Rechtsanwälte, Staad. In 2005, he has completed his habilitation at the University of St.Gallen and has been appointed lecturer at the University of St.Gallen for private law, commercial law and air law.

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.d-nb.de> abrufbar.

ISBN: 978-3-258-07242-5

Alle Rechte vorbehalten

Copyright © 2007 by Haupt Berne

Jede Art der Vervielfältigung ohne Genehmigung des Verlages ist unzulässig

Printed in Germany

[www.haupt.ch](http://www.haupt.ch)

**Vinay Kalia**  
**Roland Müller**

# **Risk Management at Board Level**

## A Practical Guide for Board Members

**HAUPT VERLAG**  
**BERN · STUTTGART · WIEN**



# Table of Contents

Foreword ..... 9

I. Introduction ..... 11

    1. General Overview ..... 11

    2. Importance of Risk Management ..... 13

        a) Help for Company ..... 13

        b) Bank Rating..... 13

        c) Insurance ..... 14

    3. Role of Board Members in Risk Management ..... 14

        a) Risk Management as a Part of Good Corporate Governance.. 14

        b) 360° Direction and Control..... 16

        c) Setting the Tone of Risk Management ..... 17

        d) Dealing Effectively with Strategic Issues..... 17

        e) Fostering Openness and Creativity ..... 18

        f) Guidelines and Policies for Risk Management ..... 18

        g) Serious and Extraordinary Decisions ..... 19

        h) Supervision of the Company Performance vis-à-vis Strategy . 19

        i) Organisation and Structure of Risk Management ..... 20

    4. Definitions and Concepts..... 22

        a) Definition of Risk and Security..... 22

        b) Definition of Risk Controlling..... 23

        c) Definition of Risk Management ..... 23

        d) Definition of Emergency Management ..... 24

        e) Definition of Crisis Management ..... 24

        f) Definition of Operational Risk Management..... 25

        g) Concept of Value-at-Risk ..... 25

|                                                                       |    |
|-----------------------------------------------------------------------|----|
| h) Concept of a Risk Map . . . . .                                    | 27 |
| i) Concept of Business Continuity Management (BCM) . . . . .          | 29 |
| 5. Risk Management Standards . . . . .                                | 31 |
| a) Committee of Sponsoring Organisations (COSO) Framework . . . . .   | 31 |
| b) Sarbanes Oxley Act . . . . .                                       | 34 |
| c) The Austrian Standards Institute Rules (ONR) . . . . .             | 35 |
| II. Development of Risk Management . . . . .                          | 39 |
| 1. Overview of the Development Stages . . . . .                       | 39 |
| a) Stage 1: New Concepts . . . . .                                    | 39 |
| b) Stage 2: Credit Risk Management . . . . .                          | 40 |
| c) Stage 3: Financial Risk Management . . . . .                       | 40 |
| d) Stage 4: Operational Risk Management . . . . .                     | 40 |
| e) Stage 5: Enterprise Risk Management . . . . .                      | 41 |
| 2. Risk Management and Corporate Governance . . . . .                 | 42 |
| a) Overview of ERM and Corporate Governance Interdependence . . . . . | 42 |
| b) The Cadbury Report . . . . .                                       | 43 |
| c) The Combined Code and Hampel Report . . . . .                      | 44 |
| d) The Turnbull Report . . . . .                                      | 45 |
| e) The King II Report . . . . .                                       | 46 |
| f) The Basel Committee Reports . . . . .                              | 47 |
| III. Driving Forces of Risk Management in Switzerland . . . . .       | 49 |
| 1. General Overview . . . . .                                         | 49 |
| 2. Law as a driving force . . . . .                                   | 50 |
| a) Importance of Several Regulations . . . . .                        | 50 |
| b) Swiss Code of Obligations . . . . .                                | 51 |
| c) Bank Regulations . . . . .                                         | 51 |
| d) German Law for Control and Transparency (KonTraG) . . . . .        | 52 |
| 3. Institutional Investors . . . . .                                  | 52 |
| 4. Impact of US Developments . . . . .                                | 53 |
| 5. Press . . . . .                                                    | 54 |
| 6. Others . . . . .                                                   | 54 |

|                                                         |    |
|---------------------------------------------------------|----|
| IV. Risk Management Implementation.....                 | 57 |
| 1. General Overview .....                               | 57 |
| 2. Objective Setting .....                              | 60 |
| a) SWOT-Analysis .....                                  | 60 |
| b) Risk Management Policy .....                         | 60 |
| c) Risk Management Guidelines/ Directives .....         | 62 |
| d) Risk Management Handbook .....                       | 62 |
| 3. Risk Identification .....                            | 63 |
| 4. Risk Assessment and Prioritisation .....             | 65 |
| 5. Risk Analysis .....                                  | 69 |
| a) Key Drivers Analysis/ Root Cause Analysis .....      | 69 |
| b) Suitable Actions to Respond to the Key Drivers ..... | 69 |
| 6. In-depth Risk Analysis .....                         | 73 |
| a) Quantification of the risks .....                    | 73 |
| 7. Action Planning .....                                | 73 |
| 8. Monitoring, Reporting and Supervision .....          | 75 |
| 9. Culture .....                                        | 79 |
| 10. Tools .....                                         | 81 |
| V. Summary and Advice .....                             | 83 |
| 1. Summary .....                                        | 83 |
| a) Key Messages .....                                   | 83 |
| b) Organisation at Board Level .....                    | 84 |
| c) Organisation at the Management Level .....           | 84 |
| d) Risk Management in the company .....                 | 85 |
| 2. Advice .....                                         | 85 |
| a) Integrated ERM .....                                 | 85 |
| b) Decision-Making Under Time Pressure .....            | 86 |
| c) Whistleblowing .....                                 | 87 |
| d) Checklists .....                                     | 88 |
| e) Advice for Small and Medium Companies .....          | 88 |
| f) Managing Impediments .....                           | 90 |
| g) Self-Appraisal .....                                 | 91 |
| h) Keep it Simple .....                                 | 92 |

|                                                                  |     |
|------------------------------------------------------------------|-----|
| Epilogue.....                                                    | 95  |
| Bibliography.....                                                | 97  |
| Appendix.....                                                    | 101 |
| 1: Checklist for Implementing Enterprise Risk Management.....    | 101 |
| 2: Risk Management Policy and Guidelines.....                    | 103 |
| 3: Internal Regulations for Risk Management Committee.....       | 116 |
| 4: Board Responsibility in Risk Management (King II Report)..... | 119 |
| 5: Risk Identification Form.....                                 | 123 |
| 6: Checklist for IT Risks.....                                   | 124 |
| 7: Whistleblowing Policy Document.....                           | 127 |
| 8: ERM Self-Appraisal Questionnaire.....                         | 131 |
| Abbreviations.....                                               | 135 |

# Foreword

By the Editor of this Series, Professor Martin Hillb  
Managing Partner, IFPM Center for Corporate Governance  
University of St. Gallen  
([www.ccg.ifpm.unisg.ch](http://www.ccg.ifpm.unisg.ch))

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

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

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

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

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

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

«An error alone is never the cause of company's collapse.» The cause often lies in the lack of an effective and systematic Risk Management function at the Board of Directors (BoD) level. Noteworthy is that:

- Risk Management is a new development in Corporate Governance.
- The new phase in Risk Management started in the 1970s with the growth of credit Risk Management.
- The Risk Management approach in the 21<sup>st</sup> century takes a holistic view of all risks concerning a company.
- The New York Stock Exchange (NYSE), through its Securities Exchange Commission (SEC), sponsored legislation such as the Sarbanes Oxley Act (SOX) to put additional and mandatory pressure on companies to manage risks on the operational and Board of Directors (BoD) levels and provide totally transparent information to shareholders.
- Essentially, small and medium companies (SMEs), and very small companies, feel that Risk Management does not have any meaning for them. However, Risk Management can be implemented even in such companies both on operational and Board of Directors (BoD) levels with great effectiveness and added value for the company.

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

St. Gallen/ Switzerland, March 2007

Martin Hilb

# I. Introduction

## 1. General Overview

Risk Management is nothing new and it is not a rocket science. It is common sense that has always prevailed and it is for everyone. Risk Management for individuals means the execution of certain actions, providing them with increased control over future events and a confidence to move forward with their interests intact despite the uncertainty of events ahead.

In an enterprise, several or a lot of individuals work together. This already leads to a bundled wish for increased control over future and risk. In addition, 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. They all want the enterprise to know their risks and to take corresponding mitigation actions. If the enterprise collects and systematically analyses its risks and takes adequate actions to mitigate them, this is the process of Risk Management. Simply put, this is Risk Management. The simpler we keep this message, the better it is for everyone involved. Making the message and its public face complex is only counterproductive as people start to perceive Risk Management as a bureaucratic and control-focused exercise. The implication of the above statement is that Risk Management is important to provide assurance to a large number of individuals to increase their certainty about their future in increasingly uncertain times. Enterprises mentioned here could be small, medium, or large. They all need Risk Management although the depth of analysis, formal processes, organisation, and resource allocation increases with an increase in size, complexity, and riskiness inherent in a given business.

All enterprises are confronted with risks. Unfortunately, risks are often recognised too late, so that neither enough time nor adequate measures are avail-

able to prevent the resultant damage from the realisation of the risk potential. To prevent this, every farsighted enterprise management should aim to recognise possible risks and to minimise as far as possible the most dangerous amongst these through adequate strategic or surgical measures. Therefore, consciously or unconsciously every enterprise management pursues Risk Management as a rule. 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.

Risk Management is an untransferable and inalienable task of the Board of Directors (BoD). 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 undelegable duty to avoid unnecessary risks and minimise inevitable risks in order to guarantee the existence and the advancement of the enterprise. Therefore according to article 663b CO from the beginning of the year 2008 all companies are forced to make a comment in the notes to the annual financial statements to the carrying out of risk assessment. To be able to compare the efficiency of such 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; and
- Objective of Risk Management.

Such Risk Management standards were introduced in the UK after comprehensive notifications were made 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 initiative have tried hard to translate this standard into practice, so that organisations and enterprises can compete within this framework.

## **2. Importance of Risk Management**

### **a) Help for Company**

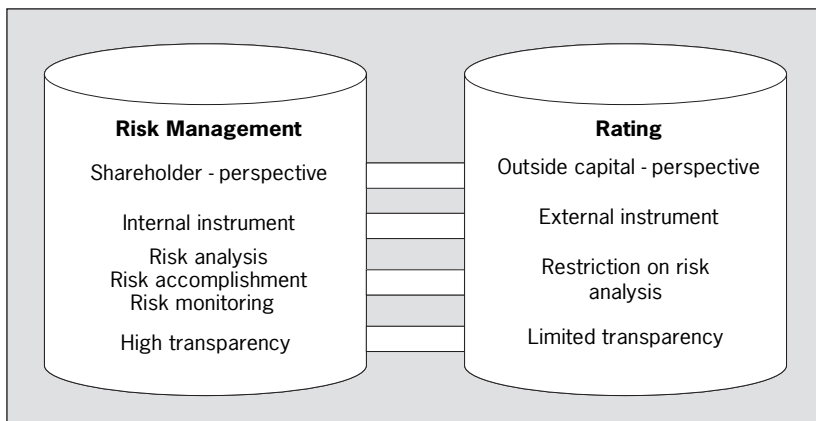
Some of the most common reasons cited for Risk Management are that it helps the company with several issues, such as:

- Formulate and develop a strategy that responds to major risks;
- Make the company risk profile transparent with respect to stakeholders;
- Assure shareholders and stakeholders that risks have been assessed and managed;
- Put in place sound early warning systems;
- Ensure that the firm is sustainable (for example, protecting it from existence-threatening situations);
- Have appropriate Risk Management solutions and control measures in place;
- Safeguard reputation and goodwill;
- Continuously increase the value of the company through proactive Risk Management;
- Standardise terminology and processes relating to risk across the organisation; and
- Adhere to both old and new laws relating to risk.

### **b) Bank Rating**

Companies have an ongoing need for capital and in the Swiss economic environment banks are one of the main creditors for the company. Increasingly, banks before lending want to analyse the risk profile and Risk Management profile of the company. The ratings of the companies are increasingly being based on their Risk Management; a good rating can help them achieve easy access to capital at favourable rates, which reduces the cost of doing business. There are several organisations, such as Standard and Poors, which provide credit ratings for companies. The link between Risk Management and rating is well described in the following figure (1).

Figure 1: Risk Management and Rating



Source: Gleissner and Fuser (2003: 178) and Gleissner et al. (2004: 105)

### c) Insurance

On the one hand, companies with good Risk Management gain cheaper access to capital; on the other hand, they also negotiate favourable deals or reduced premiums with insurance providers. One such example is that of Swiss Post. According to Mr. Affolter, Head of Insurance Risk Management, the company has maintained its pre- September 11 premiums despite a perceived overall increase in the risk environment. He asserts that this has been possible only due to sound Risk Management practices. The assertion becomes even stronger when compared to the company's competitors whose premiums have almost doubled in the same period.

This is indeed an important development as Risk Management now makes direct financial sense, contrary to the belief of many sceptics who felt Risk Management was just a cost centre and a bureaucratic exercise.

## 3. Role of Board Members in Risk Management

### a) Risk Management as a Part of Good Corporate Governance

The IFPM Center for Corporate Governance at the Institute for Leadership and Human Resource Management at the University of St. Gallen has established a Board Management School, where Directors of Boards (BoD) are

professionally trained. Discussions with the participants of different courses have resulted in a list of 10 principal BoD mistakes and deficiencies (Table 1). In the case of bankruptcies, more than one of these points can be found.

Table 1: Mistakes and Deficiencies at Board Level

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"><li>1. Wrong structure and insufficient qualification of the Board of Directors (BoD), in particular concerning the function of the Chairman combined with the absence of the non-executive Board members.</li><li>2. Board members are not sufficiently prepared and do not have the necessary overview.</li><li>3. Board decisions are influenced by conflicts of interests supported by insufficient internal regulations.</li><li>4. Missing or insufficient strategy identifications and strategy control.</li><li>5. Missing or insufficient risk management, in particular concerning liquidity planning and succession regulations.</li><li>6. Low frequency of Board meetings, so that the Board of Directors can only react to changes and events instead of being proactive.</li><li>7. Unsatisfactory provision of information and information evaluation, in particular by insufficient or delayed reporting to the Board of Directors.</li><li>8. Delayed or incorrect decision making, in particular according to incomplete decision documents.</li><li>9. Insufficient cooperation between Board of Directors and Executive Management, in particular unclear allocation of duties and competence.</li><li>10. Absence of periodic evaluation of the Board members and Executive Management; inefficient Board and Executive Board members are replaced too late.</li></ol> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Missing or insufficient Risk Management is listed here as one of the principal defects. It is astonishing knowledge that all ten principal defects lead back to Corporate Governance issues. A consistent collection of all risks linked to management would have to led to uncovering and/or in the long run to the prevention of such errors. Therefore, in the area of Corporate Governance alone, Risk Management assumes key significance for the Board of Directors (BoD). Some of the key responsibilities for the role of the Board of Directors (BoD) with regard to Risk Management are discussed in the following sections.

### b) 360° Direction and Control

If the reasons for the failure of enterprises in the past decades are analysed, then it can be clearly observed that often the Board of Directors (BoD) did not (or decided not to) recognise threatening risks and therefore did not initiate any measures to mitigate these risks. The lack of managing the resulting damage was therefore an adequate cause for the fall of the enterprise. This demonstrates that financial risks are not the only cause of failure. Strategic risks have also moved into the consciousness of BoDs in addition to the financial and operational risks identified, evaluated, and mitigated. Corporate Governance risks in particular are also part of integrated Risk Management. Figure 2 illustrates these risks as a «risk radar»:

Figure 2: 360° Overview by Risk Radar



Source: Kägi and Pauli (2003: 7)

In a similar way as described in the diagram above, the main «Risk Traps» at the Board level have been further detailed by Prof. Dubs,<sup>1</sup> who classifies the main risks for the board into the following four categories:

- Environment and Market
- Planning and Culture
- Finance and Costs
- Legal and Compliance

### **c) Setting the Tone of Risk Management**

The tone of Risk Management is set at the top of the organisation. When Risk Management is being established, it could be considered to be a costly, resource-consuming, and bureaucratic exercise. There is some truth in this assertion in situations where Risk Management is not «lived» by the organisation but is carried out to satisfy a demand issued by the Executive Board (ExB). In these cases, Risk Management could fail to achieve its objectives. To reduce the likelihood of such an outcome, the Board of Directors (BoD) can be pro-active in demanding information regarding risks, sticking to guidelines and policies (preferably championed at a senior level), and analysing the quality of Risk Management initiatives and their impact on the performance of the company. In many instances, it is reported that owing to time constraints and lack of resources, Risk Management discussions were cancelled or postponed. Especially in the early days of establishing Risk Management in the organisation, the commitment of Executive Board (ExB) sends signals across the organisation about its relative importance. Boards could address this challenge by defining Risk Management as a key contribution to company performance, rather than as the provision of information about poor performance.

### **d) Dealing Effectively with Strategic Issues**

Boards normally meet five or six times a year<sup>2</sup> and have many issues to discuss in their meetings apart from risk-related issues. This allows time only for the most critical and strategic issues. The Board of Directors (BoD) must ascer-

---

<sup>1</sup> Dubs (2006: 31)

<sup>2</sup> According to the Swiss Code of Obligations, a minimum of four meetings per year are required.

tain the categories into which risks will fall, and the level at which these risks will be dealt with in the organisation. In a workshop organised with the participation of the Board members, one critical remark was, «there should be a good understanding of the difference between *risk issues* and *management issues*». It is not possible for the Board of Directors (BoD) and the Executive Board (ExB) to deal with all issues, as the result is the dilution of the time and resources that should be committed to the most important strategic issues. Once strategic risks are known to Board members, strategies to pursue, avoid, or minimise these risks and the *risk appetite* of the company should be provided by the Board of Directors (BoD). The organisational culture (risk-averse or risk-hungry) is one determinant of the strategy that emerges.

#### **e) Fostering Openness and Creativity**

«Risks are not so polite as to knock on the door...they come from unexpected quarters and at unexpected times.»<sup>3</sup>

This remark was made during one of the Risk Management presentations. It suggests that Board of Directors (BoD) have to be proactive and imaginative in visualising the risk «landscape» and scenarios that could materialise. Such ideas cannot all be generated by senior managers. The Board's role is therefore to provide an environment in which such information can flow freely. In this regard, Prof. Dr. Boutellier of the Swiss Federal Institute of Technology (ETH Zurich) and a member of several boards remarks: «The policy of *shooting the messenger* just won't work.»<sup>4</sup> This change to democratising information-gathering and decision-making starts at Board level.

#### **f) Guidelines and Policies for Risk Management**

According to a survey,<sup>5</sup> guidelines and policies are set by the Board of Directors (BoD) in 34 percent of the companies and by the Executive Board (ExB)

---

3 This was a general comment made by a senior Board member in the Risk Management workshop organised by the author.

4 Prof. Boutellier made this remark during the Risk Management presentation to Risk Managers from across Europe in July, 2005.

5 The survey was conducted by the Transfer Center for Technology Transfer (TECTEM) at the University of St. Gallen on the theme of Enterprise Risk Management.

in more than 60 percent of the companies surveyed. 56 percent of the companies had formal Risk Management guidelines. The trend of Board of Directors (BoD) approving the guidelines and policies is, however, on the rise as boards are getting more and more involved in Risk Management. The policies and guidelines set by the Board include information about necessary processes, structure, reporting, and monitoring systems. If Risk Management expertise does not exist on the Board level, it may acquire internal or external help to establish these guidelines and policies. Appendix 2 and Appendix 3 respectively provide real life examples (anonymous) Risk Policy & Guideline document and Internal Regulations for a Risk Management Committee at the Board level.

**g) Serious and Extraordinary Decisions**

There are many examples of extraordinary events which can occur at any given time – including fire at a production unit, poisoning of a packaged food consignment, or fatalities caused by manufacturing flaw. The Board of Directors (BoD) has to ensure that a robust but flexible system is in place for training employees to effectively manage such situations and diminish the extent of negative publicity that arises from them. They also have to ensure effective communication channels, such that information reaches the Board of Directors (BoD) before it reaches the press. Such interventions constitute business continuity planning. Honesty, integrity, and transparency are often valued highly in society, though surprisingly few companies demonstrate, or live up to, these values.

**h) Supervision of the Company Performance vis-à-vis Strategy**

After establishing the guidelines, the Board of Directors (BoD) provides adequate supervision of their implementation. It reviews whether there are deviations from targets and policies, and whether the guidelines and the company risk limits are being adhered to. The challenge is for the Board of Directors (BoD) to achieve effective supervision without interfering excessively in the work of top managers. In the words of Prof. Hilb, Professor of Business Administration at the University of St. Gallen, Switzerland, «Boards have

to keep their noses in and their hands out» of company business.<sup>6</sup> Appendix 3 provides a real life example of Internal Regulations for Risk Management Committee at the Board Level providing a good insight to the supervision role as understood by the Board.

#### **i) Organisation and Structure of Risk Management**

If the Board is to «keep its nose in and hands out» of company business, it has to be able to appoint effective and committed people to the Executive Board (ExB). There are often systematic deficiencies in management that require a special focus on Risk Management. Boards can work in that direction by hiring appropriate management for the organisation. The key components of Risk Management structure in an organisation are discussed below.

- **CEO and Executive Board (ExB)**

The ultimate responsibility to execute the Risk Management policies designed by the board lies with the CEO and Executive Board (ExB). The CEO recommends the structure and management (for example, the Head of Risk Management) to the Board, and proposes guidelines and processes that could be instituted.

- **Head of Risk Management (team, committee, or an individual)**

The responsibility for implementing Risk Management could rest with a team, a committee, or an individual. Such a responsibility includes:

- Co-ordinating the Risk Management process across the entire enterprise;
- Managing the RM process;
- Identifying the «owners» of the major risks;
- Consolidating the risk-related information across the organisation and reporting it to the CEO and the Board of Directors; and
- Updating guidelines, policies and processes.

---

6 Hilb (2004: 50)

- **Risk coordinators**

Risk co-ordinators represent the Head of Risk Management (or a committee or team) at the divisional and business unit level and carry responsibilities similar to the Head of Risk Management at those levels.

- **Risk Owners**

Risk owners are responsible for specific risks. They decide on the appropriate analysis and action for managing the specific risks; they prepare appropriate reports (according to the levels at which they operate); and they decide on who would undertake actions to mitigate their risks.

- **Response Owners**

«Response owners» carry out the actions/ measures intended to mitigate key risks, and provide regular feedback on the effectiveness of those actions.

- **Risk Champions**

Normally, the Head of Risk Management and Risk Co-ordinators are risk champions in an organisation. Their responsibilities include:

- Spreading an awareness of risk and building a culture of Risk Management in the organisation;
- Providing Risk Management training and development; and
- Linking Executive Board (ExB) initiatives to the rest of the organisation.

Risk champions should have an excellent knowledge of the business, organisation, and its culture, and should have authority to move freely across the organisation. Companies may identify risk champions who are not part of the formal Risk Management organisation.

- **Auditing**

The auditing function links Risk Management to the auditing process, reporting on the diligence of the Risk Management process with critical evaluation and suggestions for improvement.

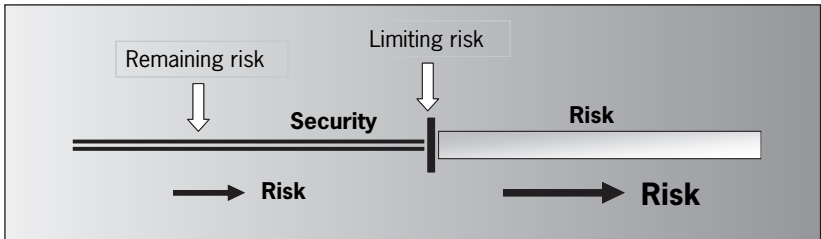
## 4. Definitions and Concepts

### a) Definition of Risk and Security

Risks are the possible deviations from the target values caused by accidental interferences due to the unpredictability of the future. The ratio between the probability of an occurrence of damages and the expected measure of damages is called individual risk. In principle, it would be possible to calculate the risk if its probability and the measure of damages were not – as a rule – indefinite parameters.

Security, on the other hand, is a situation where the remaining risk is not higher than the limiting risk. The limiting risk is the highest justifiable risk of a certain technical process or condition.

Figure 3: Risk and Security

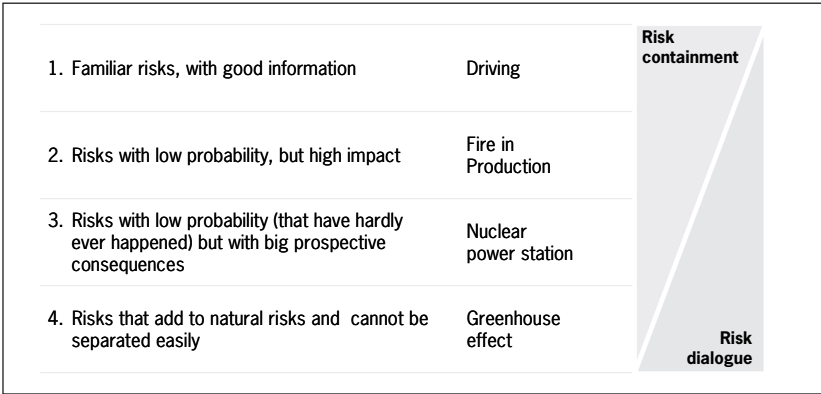


Source: Gindi (2003: 13)

According to Lewis,<sup>7</sup> there are four types of risk (see Figure 4). The strategies to deal with them range from containment to risk dialogue. The more difficult it is to quantify and ascertain risks, the more advisable it is to initiate risk dialogue to manage those risks.

<sup>7</sup> Lewis (1990)

Figure 4: Four Main Types of Risk



Source: Boutellier and Kalia (2006)

**b) Definition of Risk Controlling**

Risk controlling is a component of Risk Management and aims at the examination or adaptation of the process with changes of the enterprise or its sphere. Although risk control is a component of Risk Management, it concerns the active influencing of the recognised risks.

**c) Definition of Risk Management**

Risk Management is generally understood as the holistic process involved in recognising possible risks, and the measures undertaken to reduce and monitor them. It thus comprises a modular cycle of communication, documentation, control, early warning mechanisms, and advancement. The substantial elements of this automatic control loop are risk perception, risk identification, risk communication, risk analysis, risk evaluation, and risk monitoring.

This general definition of Risk Management as a comprehensive process can be further concretised:

«Risk Management means the permanent and systematic recording of all kinds of risks with regard to the existence and the development of the enterprise. It involves analysing and prioritising recognised risks as well as defining and implementing adequate strategic or surgical measures to minimise non-tolerable risks.»

In this definition, the following important elements are united in connection with Risk Management:

- It concerns not only a unique action, but a steady process which must be implemented in the enterprise.
- In order to not merely recognise the obvious risks, a structured procedure is necessary, aimed at investigating and listing all risks within all ranges.
- Each risk is to be judged individually and to be evaluated by the same yardsticks to establish interconnections as regards the degree and kind of risk potential involved.
- Within the scope of its risk policy, company management has to decide which risks must be accepted, avoided or managed on the basis of their consequences and suitable measures.
- The logical conversion of agreed strategic or mitigation measures to manage or reduce potential risks.
- And finally, Risk Management can only be successful if new emerging risks and claims are communicated in a standard form on all enterprise levels (so-called Risk Reporting) and if a suitable organisation exists to ensure ongoing process optimisation (so-called Risk Controlling).

#### **d) Definition of Emergency Management**

Emergency management deals with stabilising an organisation following what usually is a physical event. Thus, the Emergency Management Plan is the first plan to be executed before any other plan is invoked, including the Business Continuity Plans. In many emergencies, few real decisions need to be made, but rapid and appropriate action is required.<sup>8</sup>

#### **e) Definition of Crisis Management**

While in Emergency Management the need for action is predominant, Crisis Management calls primarily for decisions. Crisis Management is an extension of Emergency Management, both in scope and in the duration of the period its plan covers.<sup>9</sup> The Crisis Management Plan follows the Emergency Manage-

---

<sup>8</sup> Brauner (2001)

<sup>9</sup> Laye (2002)

ment Plan and includes processes for decision-making, communication, and general coordination. Its scope includes but is not limited to physical events. It may invoke:

- Business Continuity Plans as needed; and
- Disaster Recovery aims at recovering IT systems. The corresponding Disaster Recovery Plan is executed in parallel to the Business Continuity Plan(s) and is a prerequisite to return to normal operation for any IT-dependent business process.

#### **f) Definition of Operational Risk Management**

Operational risk is defined by the Basel Committee as «The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events». Operational Risk Management and line management together assess and monitor these risks and prepare risk mitigating strategies and actions. The Business Continuity Plan is a response prepared to react to a subset of operational risks, defined by the scope and size of events: The focus of Business Continuity Management is not on risks to the core-business objectives but on external risks that lie outside the competencies of the business and cause significant business disruption that might threaten the survival of the company.<sup>10</sup>

#### **g) Concept of Value-at-Risk**

In recent years, an unprecedented surge in the usage of Risk Management practices has been witnessed, with Value-at-Risk (VaR)-based Risk Management emerging as the industry standard by choice or by regulation.<sup>11</sup> As a Risk Management technique, Value-at-Risk describes the loss that can occur over a given period, at a given confidence level, due to exposure to market risk. The simplicity of the Value-at-Risk concept has directed many to recommend that it becomes a standard risk measure, not only for financial establishments involved in large-scale trading operations, but also for retail banks, insurance companies, institutional investors, and non-financial enterprises. Value-at-

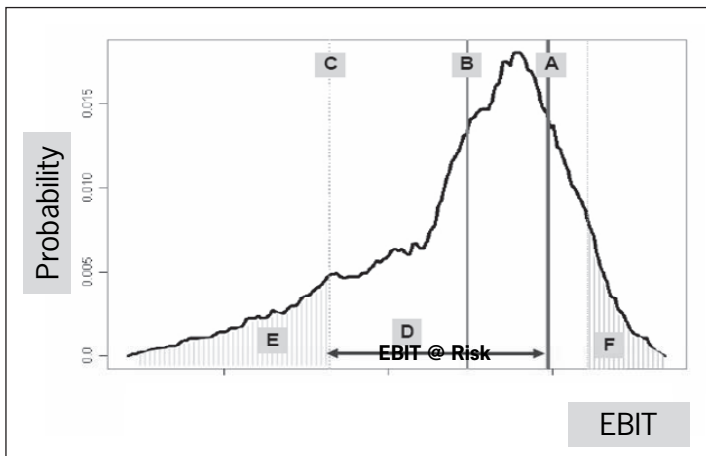
---

<sup>10</sup> McCrackan (2005a)

<sup>11</sup> Dowd (1998) and Jorion (1997)

Risk, which has achieved the high status of being written into industry regulations,<sup>12</sup> has become an inalienable tool for risk control and an integral part of methodologies that dispense of capital between various business spheres.

Figure 5: EBIT@RISK Concept



Source: Axpo Holding AG, 2005

*In the figure:*

*A is planned EBIT; B is expected EBIT based on risk considerations (systematic deviation); C is risk adjusted EBIT (minimal level) = minimal EBIT value with 90 percent probability; D is the EBIT at risk equalling the difference between planned EBIT and risk-adjusted EBIT (minimal level); E is the remaining risk of 10 percent that the company retains less than the risk-adjusted EBIT (minimal level); and F is probability of 10 percent that the company results are greater than the result risk-adjusted EBIT (minimal value).*

It suffers, however, from being unstable and difficult to work with numerically when losses are not «normally» distributed – which in fact is often the case, because loss distributions tend to exhibit «fat tails» or empirical discreteness.<sup>13</sup> Value-at-Risk (VaR) is described in J.P. Morgan's<sup>14</sup> RiskMetrics system documentation in the following way:

<sup>12</sup> Jorion (1996) and Pritsker (1997)

<sup>13</sup> Rockafellar and Uryasev (2002)

<sup>14</sup> J.P. Morgan (1995: 2)

«Value-at-Risk is an estimate, with a predefined confidence interval, of how much one can lose from holding a position over a set horizon. Potential horizons may be one day for typical trading activities or a month or longer for portfolio management. The methods described in our documentation use historical returns to forecast volatilities and correlations that are then used to estimate the market risk. These statistics can be applied across a set of asset classes covering products used by financial institutions, corporations, and institutional investors.»

While measures like VaR play an important role in quantifying risk exposure, they comprise only one piece of the Risk Management puzzle: probabilities. Probabilities are an indispensable input into the Risk Management process, but they do not determine how much risk a corporation should bear and how much risk should be hedged.

**h) Concept of a Risk Map**

Risk Mapping is the process of identifying, quantifying, and prioritising risks in relation to the achievement of business objectives. It should be linked with the business planning process. Figure 6 represents the classic Risk Map:<sup>15</sup>

Figure 6: The Classical Risk Map

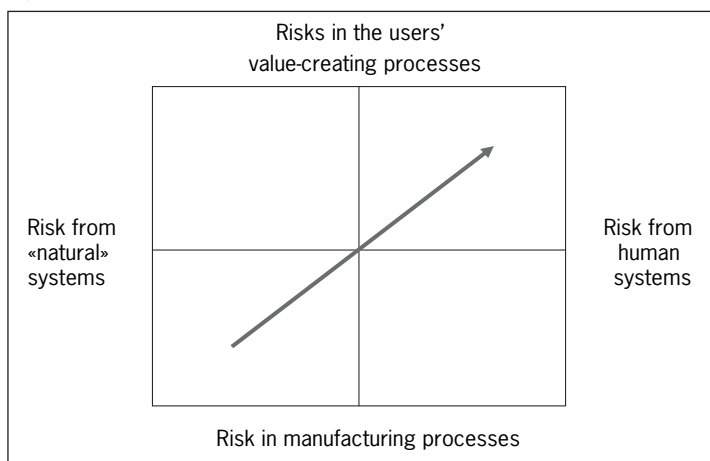


Source: Beswick and Bloodworth (2003: 2)

<sup>15</sup> Beswick and Bloodworth (2003)

The Risk Map changes in at least two ways. With new opportunities available, the nature of risk has begun to change in that risk is coming more and more from «man-made» systems not just hazards of nature. Of the above driving factors, some are «natural» but the new ones are «man-made» factors and strategic decisions (see Figure 7).

Figure 7: From Natural to Man-made Risks



Source: Ullberg et al. (2002: 472)

The arrow in the figure above illustrates how a shift in the focus of sources of risk has occurred and expanded the Risk Map and, as a consequence, the competence demands on effective Risk Management.<sup>16</sup>

Managing the new Risk Map effectively gives one the possibility of harvesting the full potential of opportunities in the knowledge or service economy. People (suppliers and users) and systems (natural and man-made) then interact in a value-creating system that leads to a change in the value-creating logic.

<sup>16</sup> Ullberg et al. (2002: 472)

### i) **Concept of Business Continuity Management (BCM)**

Once a company has developed its Risk Management, the next logical step is to move towards Business Continuity Management (BCM). BCM is concerned with developing organisation-wide resilience, allowing an organisation to survive the loss of part or all of its operational capability or a significant loss of resources. It is a relatively new discipline that originates in an evolution and fusion of already existing activities.<sup>17</sup> The plans these activities produce are related to the Business Continuity Plans including *Emergency Management, Crisis Management and Operational Risk Management* (see Section I.4).

While Business Continuity Management touches on all these management activities, it is a holistic view that starts from the continuity of business processes. The driving forces behind these activities are (external) threats. Another motivation for the introduction of Business Continuity Management can simply be the need for compliance with some regulations.<sup>18</sup> The most prominent examples are the Combined Code in the UK and the New Basel Capital Accord for banks in OECD countries.

Business Continuity Management understands the business and establishes what is vital for its survival. It is often equalled with IT disaster recovery. It is, however, a business-owned and business-driven process that unifies a broad spectrum of management disciplines. Business Continuity Management has to focus on mission critical activities.<sup>19</sup>

The key objectives of an effective Business Continuity Management strategy should be to:

- Ensure the safety of staff, maximise the defence of the organisation's reputation and brand image, minimise the impact of Business Continuity events (including crises) on customers/clients, limit/prevent impact beyond the organisation, demonstrate effective and efficient governance to the media, markets and stakeholders, protect the organisation's assets and meet insurance, legal and regulatory requirements.<sup>20</sup>

---

17 McCrackan (2005)

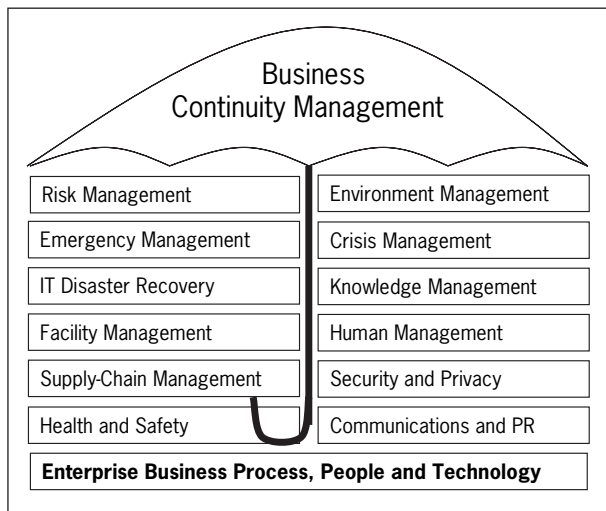
18 CMI (The Chartered Management Institute) (2005)

19 BCI (The Business Continuity Institute) (2005)

20 BCI (The Business Continuity Institute) (2005)

- Business Continuity Management is frequently<sup>21</sup> represented as an «umbrella» for other management disciplines (see Figure 8). This analogy provides a good overview of the maximum possible scope of Business Continuity Management.

Figure 8: Business Continuity Management Umbrella



Source: Decker (2004: 3)

The image certainly helps to raise the status of the Business Continuity community, and when implementing Business Continuity Management in an organisation it is tempting to deduce from it the need for an extra management layer. It is believed that Business Continuity Management will only find acceptance within a company if it builds on existing structures and efforts and complements them. For example: To build «bullet-proof» Business Continuity Management, it is imperative to understand the risks that an organisation should be prepared for. To this end, corresponding scenarios would operationalise the risks. In order to understand what it takes to impact the

21 Smith (2002) and Decker (2004: 3)

continuity of a business process, its dependencies have to be looked into. Disregarding the reasons why a certain situation has arisen, basic questions can be asked such as:

- What is needed for a process to work (in standard conditions)?
- What work-around procedures are possible if these resources are not available / limited?
- What minimum set of resources is required?
- How can these resources be acquired?

This is determined through a set of possible scenarios. Hence, only using a resource- driven approach prepares against an unreasonable set of resource-loss scenarios, which become expensive and unmanageable.

## **5. Risk Management Standards**

### **a) Committee of Sponsoring Organisations (COSO) Framework**

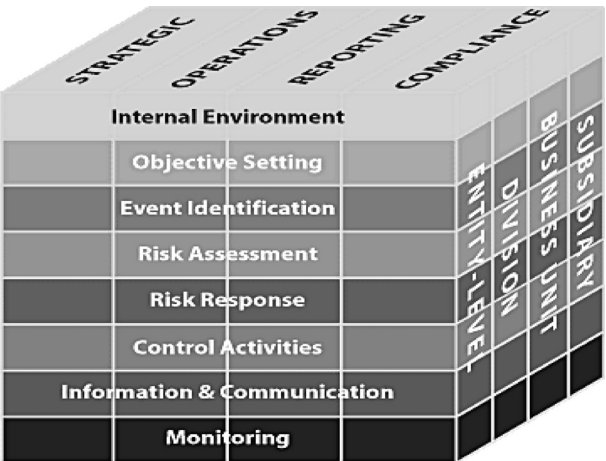
The Committee of Sponsoring Organisations (COSO) of the Treadway Commission was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector initiative which studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the US Securities and Exchange Commission (SEC) and other regulators, and for educational institutions.<sup>22</sup> The National Commission was jointly sponsored by five major professional associations in the United States, the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, The Institute of Internal Auditors, and the National Association of Accountants (now the Institute of Management Accountants). The Commission was wholly independent of each of the sponsoring organisations, and contained representatives from industry, public accounting, investment firms, and the New York Stock Exchange. COSO was the first attempt to provide a framework for Enterprise Risk Management (ERM).

---

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

The figure (9) below provides an overview of the integrated Enterprise Risk Management framework of COSO.

Figure 9: COSO Enterprise Risk Management Framework



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

COSO categorises ERM as a Process, affected by an entity’s board, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. ERM is considered important as a value-enhancing tool for companies and shareholders alike; it helps enhance value by:

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

COSO categorises the entity's objective into four categories: Strategic, Operational, Reporting, and Compliance. These activities are carried out at all organisational levels, namely Enterprise/Corporate level, Divisional level, Business Units level, and Subsidiary level. A portfolio view of risks is recommended, i.e. management tries to ascertain an entity-wide view of risk and also how risks co-relate. The framework recommends eight components for ERM, including:

- Internal Environment;
- Objective Setting;
- Event Identification;
- Risk Assessment Risk Response;
- Control Activities;
- Information and Communication; and
- Monitoring.

The eight components will not function identically in every entity. Application in small and mid-size entities, for example, may be less formal and less structured. Nonetheless, small entities can still have effective Enterprise Risk Management, as long as each of the components is present and functions properly.

COSO specifically suggests that management is accountable to the Board, which provides governance, guidance, and supervision. By selecting management, the Board of Directors (BoD) has a major role in defining what it expects as regards integrity and ethical values; it can confirm its expectations through supervisory activities. Similarly, by reserving decision-making authority as regards specific key decisions, the Board of Directors (BoD) plays a role in mapping out strategy, formulating high-level objectives, and undertaking broad-based resource allocation. The board provides supervision with regard to Enterprise Risk Management 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 entity's risk appetite; and

- Appraising the most significant risks and checking whether management is responding appropriately.

#### **b) Sarbanes Oxley Act**

Sarbanes Oxley Act is in fact not a specific Risk Management framework or regulation. On the surface, it is more of a regulation to improve internal controls and financial reporting. Signed into law by President George W. Bush in July 2003, the Sarbanes-Oxley legislation<sup>23</sup> turns the spotlight on Corporate Governance and aims to reduce the chances of another debacle like Enron.<sup>24</sup>

The new rules apply to all companies listed on a US stock exchange – including those headquartered overseas whose shares are traded as American Depositary Receipts (ADRs) – and make it mandatory for them to demonstrate that they have proper controls in place.<sup>25</sup> Other areas of SOX cover ethical behaviour, Board composition, and the independence of auditors. Senior executives are deemed personally responsible for compliance and must testify to the accuracy of their companies' accounts.

Organisations are often fooled into thinking Sarbanes Oxley is simply a technology challenge and that installing one piece of software is the panacea. Three recent developments highlight the fact that compliance and Risk Management systems have not been effective and that increased attention will be focused on them in the future. These are:

- The amendment 2004 to the US Sentencing Guidelines<sup>26</sup>;
- The exposure draft of an enterprise Risk Management Framework by the Committee of Sponsoring Organisations (COSO) of the Tread way Commission; and
- The Audit Standard for Audits of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements, released by the Public Company Accounting Oversight Board (PCAOB) on March 9, 2004.

---

23 SOX (Sarbanes Oxley Act) (2002)

24 Labaton and Oppel (2002: A1)

25 Section 404 forces the companies to establish and maintain adequate internal control structures and procedures for financial reporting but it is being interpreted as a requirement of Risk Management.

26 Kimmich (2006: 25)

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.

### **c) The Austrian Standards Institute Rules (ONR)**

The Austrian Standards Institute (ON) in 2005 started an initiative to create rules on Risk Management for organisations and systems. These were prepared by the workshop AK 1113 «Risk Management» set up by the Austrian Standards Institute on the one hand, and by the Technical Group «Risk Management» of the Swiss Association for Quality (SAQ). These are now called the ONR rules. These rules have gone a step further than the other contemporary standards and frameworks in the sense that it is the only report which is not only about presenting terminologies and a general wish list of Risk Management processes but also about providing detailed methodologies for assessing treating and controlling risks. It also explains how Risk Management is integrated into an existing system of organisation. The report is divided into five parts (ON Rule 49000, ON Rule 49001, ON Rule 49002-1<sup>27</sup>, ON Rule 49002-2, and ON Rule 49003<sup>28</sup>). It provides information on:

- Terms and principles;
- Elements of Risk Management system;
- Guidelines for Risk Management;
- Guidelines for the integration of Risk Management into the general management system; and
- Qualifications of the risk manager.

---

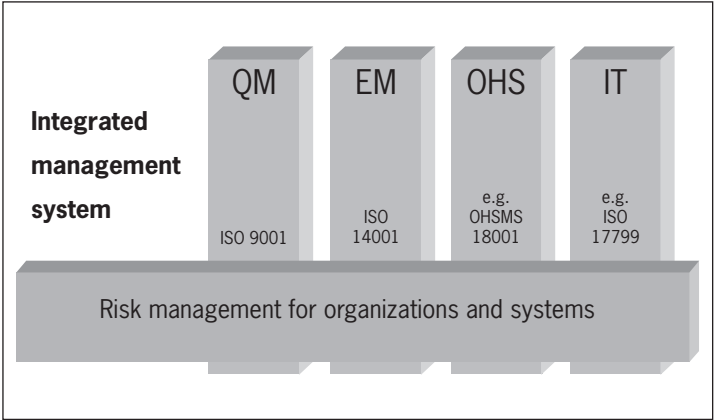
27 ONR 49002-1 (2004)

28 ON Rule 49003 (2004)

The rules of this report at present are not obligatory but many experts interviewed are of the opinion that as was the case with ISO Quality Management and others, i.e. from being non-obligatory they became the standard norms, it might be possible that these ON Rules also in time become a standard for the industries at least in the Swiss and Austrian region. For this reason, the ON Rules have serious implications.

The report suggests bringing Quality management QM (ISO 9001 and ISO 9004), Environmental Management (EM) (ISO 14001), Occupational Health and Safety OHS (OHSMS 180001, 1999), and IT security IT (IS 17799) under one umbrella, and that the Integrated management system and Risk Management should run through this system to be effective<sup>29</sup> (see Figure 10).

Figure 10: ONR Proposes Integration of Various Quality Standards for ERM



Source: ONR 49000 (2004: 13)

It is also suggested that as a management tool, Risk Management should interact with other management tools, in particular planning, controlling, internal control systems, and external auditing as shown in Table 2.

29 ONR 49000 (2004: 12)

Table 2: Interaction of Risk Management with other Management Tools

|                                      | <b>Function</b>                                                                                                               | <b>Interface Function to risk management</b>                                                                                                                                          |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Planning                             | Assessment of the situation, vision, mission, definition of objectives, strategies and allocation of resources                | Definition of risk policy, weighing chances and risks when selecting objectives and strategies                                                                                        |
| Controlling, internal control system | Coordination of planning with the results, provision of information for control and coordination; focus: financial management | Early-warning system to identify where the results can differ from plans and objectives; risk control, risk treatment, risk monitoring, quantification of the risk situation required |
| External auditing                    | Audit of annual financial statements and compliance with legal requirements or further accountancy regulations, independence  | Examination of the existence of a risk management system, maybe also of correspondence between the risk assessment and the actual economic conditions                                 |

Source: ONR 49000 (2004: 15)

One of the most important initiatives that the ONR report undertakes is that it begins addressing the issue of quantitative evaluation of risks. The issue is important but difficult as many of the risks identified have low probabilities and very little historical data is available; these are the two important ingredients required to make quantitative predictions. This is the only report that consolidates present Risk Management techniques.



# II. Development of Risk Management

## 1. Overview of the Development Stages

The development of Risk Management can be divided into five 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); and
- Stage 5 Enterprise Risk Management, i.e. taking a 360° view of Risk Management by integrating Risk Management across functions and divisions (2000 onwards).

### a) 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 insurance.<sup>30</sup> According to Haller,<sup>31</sup> Frank Knight, 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, Congress passed the McCarran-Ferguson Act, delegating the regulation of insurance to the various states.<sup>32</sup>

---

30 Haller (1999)

31 Haller (1999)

32 Kloman (1999: 12)

#### **b) Stage 2: Credit Risk Management**

*Stage two* occurred during the 1970s with the focus on insurance management, i.e. the co-ordination of pure insurance, which could be considered as traditional risk transfer.<sup>33</sup> Important landmarks in Risk Management in these years were the foundation of some associations with Risk Management in their sights, 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»<sup>34</sup> 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.

#### **c) 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.<sup>35</sup> October 19, 1997 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.

#### **d) 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.<sup>36</sup> The term Chief Risk Officer (CRO) was for the first time used by James Lam at GE Cap-

---

33 Haller (1999)

34 Kloman (1999: 12)

35 Haller (1999)

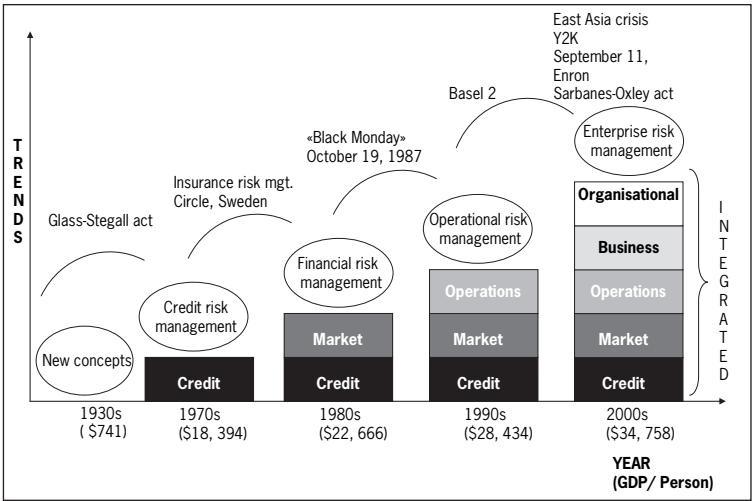
36 Haller (1999)

ital describing the function of CRO to manage all aspects of risk.

**e) Stage 5: Enterprise Risk Management**

The 9/11 terrorist attack on the World Trade Centre, New York<sup>37</sup> 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.<sup>38</sup> 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 given rise to concepts of Business Continuity Management where companies make sure that they survive even extreme events such as terrorism, natural disasters, epidemics, and major failures. Figure (11) provides a graphic view of these developments.

Figure 11: Evolution of Risk Management



Source: Adapted from various sources

37 Ernst & Young (2002)

38 Ernst & Young (2002)

The interesting thing to observe in this figure is that the growing affluence of the world 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.

## **2. Risk Management and Corporate Governance**

### **a) Overview of ERM and Corporate Governance Interdependence**

The task of the Board of Directors (BoD) and the Executive Board (ExB) is to define an integrated, future-oriented Risk Management concept; one which is integrated with the existing planning and a leadership process, which is equally directed at realising opportunities and yet does not constrain entrepreneurial freedom. The role of the Board of Directors (BoD) in Risk Management is similar to their role with regard to strategy, i.e. to determine the strategic risk objectives and to guarantee focused, operational Risk Management practices at management level.<sup>39</sup> At the Board level, Risk Management deals with the «process of early detection, prevention, and management of dangers as well as identification and effective realisation of entrepreneurial opportunities»<sup>40</sup>. Hilb<sup>41</sup> provides a spiral approach as a starting point for Risk Management at the Board of Directors (BoD) level (see Figure 12).

It is astonishing to note that even though some well-established Corporate Governance principles from around the world have laid much emphasis on the Risk Management role of Board members, Swiss Stock Exchange (SWX) codes<sup>42</sup> and the Organisation for Economic Co-operation and Development (OECD) Principles<sup>43</sup> do not bring Risk Management responsibilities into explicit view. There are only minor references to the subject. This deserves attention as having sound Risk Management can improve many other aspects of Corporate Governance as well, such as succession planning, strategy control, and independent supervision.

---

39 Hilb (2005: 166)

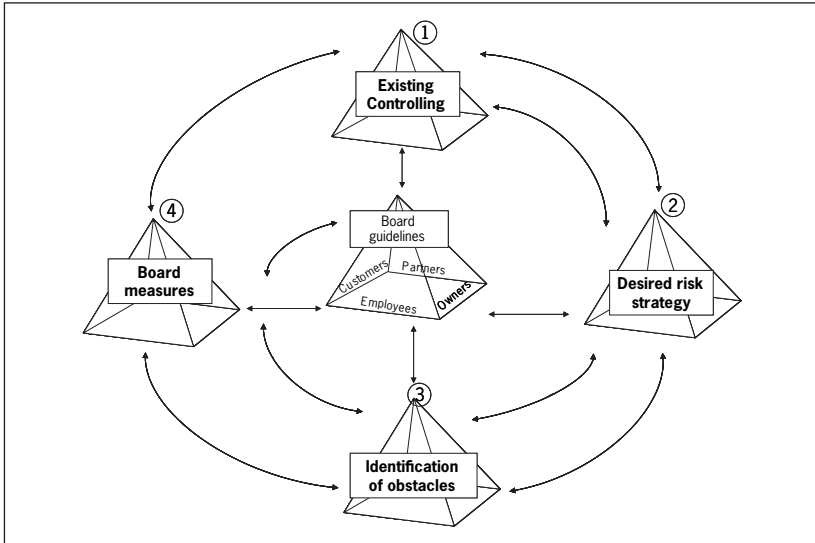
40 Ernst & Young (2002a: 7)

41 Hilb (2005: 167)

42 SWX (Swiss Stock Exchange) (2002)

43 OECD (2003)

Figure 12: Spiral Approach to Risk Management at Board Level



Source: Hilb (2005: 167)

### b) The Cadbury Report

In the UK, the «Code of Best Practice» report for Corporate Governance, published by the Cadbury Committee in 1992, was generally well received. Even though the recommendations of the report are not mandatory, all accounts of UK quoted companies now clearly state whether they follow the code or not. If not, they have to explain their reasons for not doing so.<sup>44</sup> The Cadbury Report focuses on the role of corporate directors as a unified board as well as individually. The need to implement rigorous reporting and control measures is clearly stated. AIRMIC (the Association of Insurance and Risk Managers in Industry and Commerce) in its *Guide for Insurance and Risk Managers*<sup>45</sup> chose to emphasise the implicit mandate for Risk Management.<sup>46</sup> Citing sections 4.23

44 Cadbury Report (1992)

45 Guide for Insurance and Risk Managers (1996)

46 Drennan and Beck (2001)

/ 4.24 of the Cadbury Report, AIRMIC noted that boards were now required to have a formal schedule of matters specifically reserved to them, including Risk Management policies. AIRMIC's guide further highlighted Section 4.31, which obliged directors to maintain a system of internal control through procedures designed to minimise the risk of fraud. According to AIRMIC's interpretation, the responsibilities of boards extended to include the full spectrum of legal requirements and regulations applicable to the organisation. These would encompass health and safety and environmental regulations, consumer protection laws, and a wide variety of industry-specific requirements.

In addition to this critical point of view, the Cadbury report also points out the importance of the three cornerstones of Risk Management: identification, evaluation and control. It also points out – in addition to the static Risk Management programmes – the need for dynamic programmes which help to ensure «that all future capital investment projects and production changes are methodically assessed against all conceivable risks before financial authorisation is granted.»<sup>47</sup>

### **c) The Combined Code and Hampel Report**

The combined codes of 1998 and 2003<sup>48</sup> are developed on the basis of the Hampel Report,<sup>49</sup> which was the pioneer report in introducing risk and control dimensions into Corporate Governance. Hampel widened the concept of internal control to address «business risk assessment and response, financial management, compliance with laws and regulations and the safeguarding of assets, including the minimising of fraud.»<sup>50</sup> Moreover, the report's authors explicitly stated that «we are not concerned only with the financial aspects of governance.»<sup>51</sup> Hampel took a wide view of internal control, arguing that directors should have responsibility for all aspects of control and a duty to establish a robust system of Risk Management, designed to identify and evaluate potential risks in every aspect of the business operation. This reflected

---

47 EQE (2002)

48 Combined Code (2003)

49 Hampel (1998)

50 Hampel (1998: 53-54)

51 Hampel (1998: 53)

the growing recognition that breakdowns in non-financial areas could have significant financial repercussions for companies.

These reports, however, fell short of providing guidelines for carrying out these suggestions. This shortcoming paved the way for the next report on guidelines, the Turnbull Report.

#### **d) The Turnbull Report**

Instead of defining the characteristics of an effective internal control system, the Turnbull Report takes the existence of a rigorous corporate Risk Management system as indicative of effective internal control. In this context, the Report states that «a company's system of internal control has a key role in the management of risks that are significant to the fulfilment of its business objectives. A sound system of internal control, contributes to safeguarding the shareholders' investment and the company's assets.»<sup>52</sup>

This focus on internal control is tied to the concept of a dynamic company, which requires continuous monitoring and auditing. The Report states that:

A company's objectives, its internal organisation and the environment in which it operates are continually evolving and, as a result, the risks it faces are continually changing. A sound system of internal control therefore depends on a thorough and regular evaluation of the nature and extent of the risks to which the company is exposed. Since profits are in part the reward for successful risk-taking in business, the purpose of internal control is to help manage and control risk appropriately rather than to eliminate it.<sup>53</sup>

Published in 1999,<sup>54</sup> the guidelines were formulated to help the directors of listed companies set up a sound internal control system to manage significant risks facing their business. The issues covered included the type of risks to be controlled, the control systems which were needed, the way to keep the control systems up-to-date and the responsibilities of the directors. The guidelines focused on any risk significant to business varying from company to company and suggesting various risks that a company could face, ranging from market risk, credit risk, liquidity risk, technological risk, legal risk,

---

52 ICAEW (Institute of Chartered Accountants in England & Wales) (1999: 4, para.10)

53 ICAEW (1999, p.5, para.13)

54 The Turnbull Report (1999)

health risk, safety risk, environmental risk, reputation risk, and business probity risks. The report also strongly favoured sound internal control systems in reducing and avoiding risks though admitting that not all risks can be controlled.

The Turnbull approach, accordingly, has been interpreted as involving three steps. Firstly, the Board of Directors (BoD) or relevant Board Committee members have to identify the key risks and assess how they have been evaluated and managed. Secondly, the Board of Directors (BoD) has to assess the effectiveness of the internal control system in place with a particular focus on the weaknesses and trouble spots, as identified earlier. Finally, the Board of Directors (BoD) must ensure that company reports cover all aspects of the internal control system, its procedures and its effectiveness.<sup>55</sup>

External auditors then have a part to play in Turnbull's integrated approach to managing risk, as they apply external standards to financial reporting and internal control matters

#### **e) The King II Report**

In South Africa, the release of the second King Committee Report (King II Report) in July 2001 has led for the first time to an official consideration about the importance of risk management. This report provides the most comprehensive and detailed study about the Risk Management committees at the Board of Directors (BoD) level. According to the King II Report, Corporate Governance can be seen as a company's strategic response to the need to assume prudent risks, appropriately mitigated, in exchange for measurable awards. The Board of Directors (BoD) must decide the company's appetite for risk-operations in every respect. While Risk Management should be practised throughout the company by all staff in their day-to-day activities, it is ultimately the board's responsibility to determine the level of risk it is willing to take in pursuing growth and maximising opportunities. The mechanism for controlling or minimising risk is internal control and should be embedded in the daily company activities, such as creating business plans, budgets, and undertaking other operations. The Board of Directors (BoD) should focus on

---

55 Drennan and Beck (2001)

Risk Management and internal control to safeguard the company's interests, support business objectives and sustainability, support business sustainability under normal as well as under adverse operating conditions and behave responsibly towards all stakeholders having a legitimate interest.

The risk according to this report should be viewed from three perspectives: opportunity, uncertainty, and hazard. There are many recommendations for the Board of Directors (BoD) regarding controls and reporting procedures, such as the extent of information companies should provide in their annual reports about the inculcation of Risk Management culture, the building of infrastructure, the level of unacceptable risk, the categories of business risks identified and evaluated, and the manner and frequency in which significant risks are reported to the Board.

There is a specific section dedicated to the Risk Management committee at the Board of Directors (BoD) level, which has recommendations regarding the constitution, membership (specially recommending the non-executive director to be the chairperson of this committee), terms of reference, kind of risks that can be covered, meetings, proceedings, remuneration criteria, and also general activities of this committee. The relevant and most important extracts of the King II Report are provided in Appendix 4.

#### **f) The Basel Committee Reports**

The Basel Committee 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 serious disturbances in international currencies providing a forum for regular co-operation between its member countries.<sup>56</sup> 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, by amendment in 1995, included that the senior management has to be responsible in managing credit risks arising through exposures in derivative products and other add-on factors.<sup>57</sup> Market

---

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

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

risk was added to that accord in 1996 arising from the bank's open positions in foreign exchange, trade debt securities, equities, commodities, and options. In 1998, the committee included operations risk in its agenda<sup>58</sup> 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 been established and various issues relating to defining operational risk, measurement, risk 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 such as legal risks.

Basel II signifies merely the newly formulated conditions to issue high value loans. The fact is that the regulation of Basel II has only an indirect radiating effect on enterprises.<sup>59</sup>

---

58 Basel Report (1998)

59 Gietl and Lobinger (2006: 13)

# III. Driving Forces of Risk Management in Switzerland

## 1. General Overview

**The three important characteristics of the Swiss Boards<sup>60</sup> with respect to Risk Management are:**

- The Board of Directors (BoD) has a collective responsibility in decision-making in the company. This means that the BoD has to find optimum solutions for the company as a group.
- The Board of Directors (BoD) is responsible for defining the strategy of the organisation in Switzerland.
- The Board of Directors (BoD) has to provide reasonable assurance to the shareholders and stakeholders that the key risks are being managed reasonably well in the organisation. This means that the strategic objectives of the company are attainable and all the main obstacles (risks) are being efficiently managed. This also clarifies the point that the Board of Directors (BoD) is mainly concerned with the corporate level or strategic risks and should be well aware of all the key risks facing the organisation.

The survey on Swiss companies, conducted by KPMG and the University of St. Gallen,<sup>61</sup> shows that several areas contribute to effective Corporate Governance, including information policy, finance, Risk Management, Internal Controls and internal and external auditing. These functions together provide an assurance of well being to the Board and shareholders.

---

<sup>60</sup> Müller and Volkart (2002)

<sup>61</sup> Ruud and Bodenmann (2002)

According to one of the studies, the main goal of Corporate Governance in Switzerland is safeguarding shareholders' interest.<sup>62</sup> It also suggests the most critical improvements required in Switzerland, specified as making transparent the Corporate Governance approach in companies. Most works in the field of Corporate Governance consist only of recommendations how companies should best organise Corporate Governance, such as making recommendations to shareholders' rights, to general meetings, the organisation of the Board of Directors (BoD) and the Executive Board (ExB), internal as well as external auditing, and the handling of conflicts of interest. Only a part of the Corporate Governance framework is directly and irreversibly regulated by law. Especially Swiss stock corporation law provides companies with a lot of freedom. For the first time, the code now provides recommendations as to how companies should organise their Executive Board (ExB) within compulsory legislation. Secondly, investors, especially institutional ones, are paying more and more attention to the extent to which companies stick to such Corporate Governance standards.

Switzerland has historically been, to a certain extent at least, relaxed in the field of Corporate Governance.<sup>63</sup> Recently, however, many forces have put pressure on companies to improve Corporate Governance and hence also Risk Management (implicitly). The key drivers of Risk Management in Switzerland are discussed in the next sections.

## **2. Law as a driving force**

### **a) Importance of Several Regulations**

Law is one of the main forces in enforcing better Corporate Governance practices in Switzerland, including Risk Management.<sup>64</sup> The law has been largely unchanged since 1936 with reforms in 1968 and 1992. More specifically, the Stock Exchange Act, which entered into force on January 1, 1996, has a strong influence on enforcing Corporate Governance best practices. The code of obligations now even puts more pressure on Swiss companies (both listed and non-listed) to increase transparency, auditing and compensation disclo-

---

62 Giger (2002)

63 Monks and Minow (1995)

64 Wyler (1994)

tures. Many of these developments have occurred along the lines of the Sarbanes Oxley Act.<sup>65</sup>

#### **b) Swiss Code of Obligations**

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 undelegable duty to avoid unnecessary risks and minimise inevitable risks in order to guarantee the existence and the advancement of the enterprise. The Board of Directors (BoD) has to therefore specify the risk appetite of the enterprise and the risk controlling policies. The risk goals should be aligned with a given company's strategic business objectives. Supported by article 716b OR and/or an appropriate statutory authorisation clause, the Board of Directors (BoD) can delegate, by means of decree, operational Risk Management to the management. In addition, a Chief Risk Officer (CRO) is not required, as in large-scale enterprises. It is enough if managers themselves are entrusted with Risk Management tasks, or a subordinate management member.

#### **c) Bank Regulations**

Article 9 para. 2 of BankV<sup>66</sup> regulates the fundamentals of Risk Management for banks as well as the competencies and procedures for the inclusion of business risks in internal guidelines and regulations. Accordingly, banks are required to seize, limit, and supervise in particular market –, credit –, loss –, transaction –, liquidities and image risks as well as operational and legal risks.

In 1996, the Swiss Bankers Association adopted guidelines for Risk Management in trade and derivatives. Even if the management of derivatives rescues special risks, the Risk Management principles established by the Bankers Association also are of interest at this point:

On 2 March 2000,<sup>67</sup> the Swiss Federal Court took a decision in connection with the penal procedure against the director of a bank on account of disloyal

---

65 SOX (Sarbanes Oxley Act) (2002)

66 Banks and Saving Banks Regulation (SR 952.02)

67 Unpublished Federal Court decision 6S.605/1999

management. The court ruling contains interesting explanations in view of management responsibility s regards Risk Management. Under consideration 4.a) bb) in this decision, the following implementation has been described: The accused executive officer concerned argues that it is common knowledge that in a bank the Board of Directors is responsible for setting the risk policy and the supervision of risks. One of the main tasks of the Board Committee in this bank was Risk Management. Indisputably, the decision about the loan presentations was taken by this Board committee. Therefore, the executive officers of the bank should not be accused of taking a decision which should have been taken by the Board committee.

The statement concerning Risk Management is basically accurate, but in this case was not helpful to the executive officer. Therefore, it is not surprising that in such cases both management and the Board of Directors is held to account under civil and criminal law.

#### **d) German Law for Control and Transparency (KonTraG)**

This law<sup>68</sup> has been in force since May 1998. The subsequent amendment (91 lit. c) makes it mandatory for the Executive Board to take adequate measures, especially to implement a supervising system, and to recognise early developments which could pose a risk for the further existence of the company. Many of the discussions about including risk disclosure in Swiss law have been influenced by this German precedent, including Art. 663b E-OR and amendment 728A E-OR.

### **3. Institutional Investors**

Institutional investors, especially pension funds, have been very influential and were one of the first forces in Switzerland to raise their voice for better Corporate Governance and for safeguarding shareholders' interests (i.e. Risk Management). The name which deserves special mention is the *Swiss Investment Foundation for Sustainable Development* (also known as *Ethosfunds*). The Swiss Investment Foundation for Sustainable Development was founded in 1997 by two Geneva-based pension funds and now comprises more than

---

68 Bundestagsdrucksache 13/10038 (4<sup>th</sup> March, 1998)

90 Pension Funds from all over Switzerland.<sup>69</sup> Their aim is to invest in companies which contribute to sustainable development, to send signals to the market to that effect, and to enable members to exercise shareholder rights in a responsible manner and keep a vigil on Corporate Governance in invested companies. Since the money invested in these funds is the pension savings of the ageing population, it is politically very sensitive; fund managers have no margin of error and tend to generally invest only in those companies which manage their risks in an exemplary way and provide accurate and transparent risk-related information.

#### **4. Impact of US Developments**

Shareholders of large companies involving assets of institutional investors and pension funds want increased assurance and better predictability for the performance of their funds. Non-performance can have life-altering impact on millions of lives around the world. As a result, public-listed companies are under increasing pressure to install sound Risk Management and predictability mechanisms. This is especially the case for New York Stock Exchange (NYSE) listed companies as some of the world's largest corporate disasters in the past few years have happened in the US. The Security and Exchange Commission (SEC) and the US government responded by enacting new acts and regulations, most particularly the Sarbanes Oxley Act (SOX).

According to Pfyffer,<sup>70</sup> there is also great impact of SOX on Swiss Corporate Governance and law as some elements of SOX are being incorporated in Swiss requirements owing to investors' pressure, perceived economic benefits, and requirements made by Basel II type regulations and rating agencies. The following table (3) shows how Swiss rules and regulations have been affected by SOX and New York Stock Exchange regulations.

---

69 Ethosfund (2005)

70 Pfyffer (2005)

Table 3: SOX and Swiss Law: A Comparison

| <b>Sarbanes - Oxley Act Section 301</b> | <b>Swiss Rules</b>                                                                                                                     |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Sarbanes - Oxley Act Section 301        | Swiss Code of Best Practice for Corporate Governance, par. 23                                                                          |
| NYSE Section 303 A(7)(d)                | Mandatory for banks (Swiss Federal Banking Commission Circulars 95/1)<br>Swiss Code of Best Practice for Corporate Governance, par. 19 |
| NYSE Section 303 A(7)(c) (iii) (D)      | Draft article 663b Ziff12 CO Swiss Code of Best Practice for Corporate Governance, par. 19                                             |
| Sarbanes - Oxley Act Section 404        | Article 716a CO new article 728a CO                                                                                                    |

Source: Pfyffer (2005)

## 5. Press

With the worldwide interest in Corporate Governance growing in the light of so many scandals and failures, the press in Switzerland has also played a significant role in bringing the issue to the focus of the public and politicians, making it one of the most hotly debated topics in the business polity today. Issues such as Y2K, Mad Cow disease (BSE), Severe Acute Respiratory Syndrome (SARS), September 11 terrorist attack, Corporate Scandals (Swiss air, Enron, Swiss Banking Scandals<sup>71</sup>) have been well publicised, creating increased awareness among society and businesses of risks and Risk Management.

## 6. Others

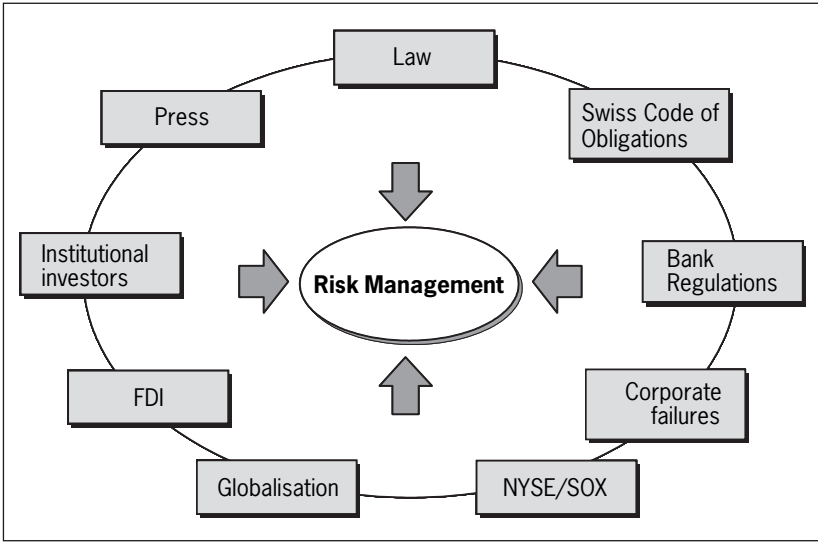
There are also other forces which are rapidly changing the face of Corporate Governance in Switzerland as was clear from the literature review, such as corporate scandals, FDI, globalisation, and others. The impact of develop-

71 Bankruptcy of Spar+Leihkasse Thun in 1991, liquidated only after 14 years in 2006. Erb Gruppe (after the Swissair disaster, Erb Gruppe is the biggest bankruptcy in Switzerland. Insolvency occurred in 2004. There were 85 companies in the group.)

ments in other countries (for example, Sarbanes-Oxley Act in the US) is also providing an impetus towards Risk Management.

Forces shaping Corporate Governance and Risk Management (RM) in Switzerland are depicted in Figure 13.

Figure 13: Forces Fostering Better Risk Management in Switzerland





# IV. Risk Management Implementation

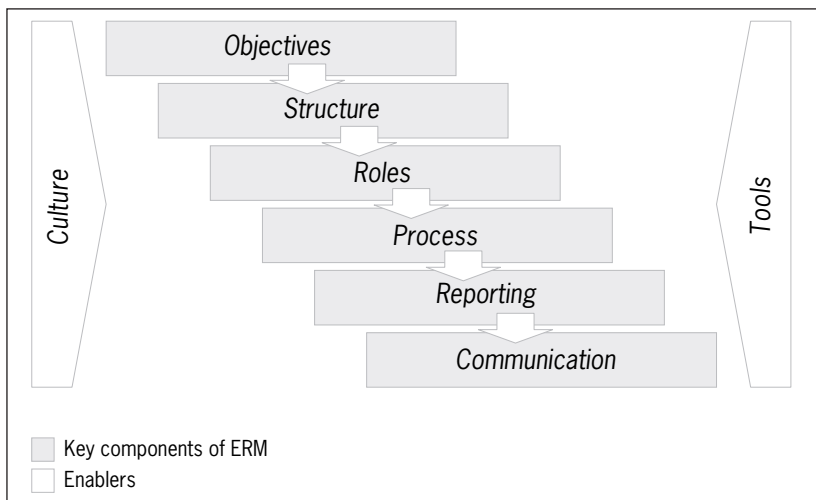
## 1. General Overview

After understanding Risk Management and its development, the status of Risk Management in Switzerland, other related concepts, and the role of the Board of Directors (BoD), it is important to know how Risk Management can be implemented in the company. The steps for this implementation and the related time plan are listed in the form of a checklist in Appendix 1. The Board of Directors (BoD) has the role of providing the strategic direction and control but should have a clear overview of how Risk Management is being carried out across the organisation. The overview has to be provided by the Board through policies and guidelines. There are some basic pre-requisite conditions that have to be fulfilled in order to achieve effective Risk Management in an organisation. These prerequisites can be divided into two categories (see Figure 14):

*Category 1: Key Components*, i.e. the elements that are directly linked to the Risk Management structure and process in an organisation, including objectives, structure, roles, processes, reporting, and communication; and

*Category 2: Enablers*, i.e. the elements that enable Risk Management components to exist and function optimally in an organisation, which includes culture and tools.

Figure 14: ERM Conceptual Framework



Source: Kalia (2006)

*Objectives:* Risk Management is more likely to be effective if it is incorporated into policies that provide direction for the whole organisation, and if it is expressed in the form of a vision, mission, and set of Risk Management objectives.

*Structure:* Risk Management is more likely to be effective if it is translated into a set of decision making routines, and implemented through Risk Management sub-structures designed for that purpose.

*Roles:* The Board of Directors (BoD) and Executive Board (ExB) have the ultimate responsibility for Risk Management. However, they need certain roles which have to be fulfilled by other people or entities if they are to be effective in managing risk. The most common roles in ERM prevalent today are those of Risk Manager, Risk Coordinators, Risk Owners, and Risk Champions. The Board of Directors (BoD) members, CEO and other members of the Executive Board (ExB) also have additional responsibility in relation to Risk Management.

*Process:* Important Risk Management processes include:

- Setting Risk Management objectives in accordance with corporate strategy;
- Identifying risks;
- Assessing the risks identified using qualitative and quantitative techniques;
- Analysing the risks;
- Planning risk mitigating actions;
- Monitoring the implementation of risk mitigation actions; and
- Providing feedback to various stakeholders about the internal and external risk environment.

*Reporting:* Reporting constitutes one of the main control activities for supervising the Risk Management process in an organisation. Good reporting systems and practices allow the evaluation of decisions that are made, and of their consequences, thereby facilitating the continuous improvement of Risk Management in the organisation. Communication and reporting processes should be made as simple as possible to avoid redundancies and to avoid turning Risk Management into a bureaucratic exercise.

*Communication:* Since one of the purposes of Risk Management is to increase transparency, communication to all relevant stakeholders is important. Communication channels include annual reports, internal reports, seminars, and management meetings.

*Culture:* Spreading a positive Risk Management culture in the organisation is an important but difficult responsibility of the Board of Directors (BoD). A primary influence on organisational culture is the formal and informal communication between members of the Board of Directors (BoD), senior managers and other employees. Risk champions and Risk Management specialists that have access to a wide range of employees in the organisation can also be important determinants of the Risk Management culture in the organisation.

*Tools:* There are several tools available for the Board of Directors (BoD) and Executive Board (ExB) to manage risks effectively. These tools fall into three categories:

- Organisational setting and strategy formulation and development tools;
- Risk Management tools; and
- IT tools.

IT tools are particularly important for managing risk-related information, for carrying out quantitative analysis of such data, and for generating risk reports.

In the next sections, a detailed analysis of the key steps of ERM Process and how they should be carried out in the organisation is presented.

## **2. Objective Setting**

### **a) SWOT-Analysis**

Starting with SWOT – analysis, risks and opportunities can be identified and assessed in an enterprise. As long as the objectives are not clear, risks cannot be defined either. Thus, every risk reflection begins with a clarification of the enterprise's objectives. They arise from the strategy, but also from the mission and the vision of the company. In this step, the organisation sets out its strategic objectives based on its Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis.

Based on corporate strategy, the Board of Directors (BoD) has to initiate the creation of the following documents to showcase the objectives, structure, and procedures to manage risk:

- Risk Management policy;
- Risk Management directives; and
- Risk Management handbook.

### **b) Risk Management Policy**

The Risk Management policy should be a brief document (2-3 pages) which is signed by the Board of Directors (BoD) responsible and the CEO (an example of Risk Management Internal Regulations for Risk Management Committee at the Board Level is provided in Appendix 3). It should provide:

- Overview of vision and mission of the organisation;
- Key strategies of the company. Some companies try to keep the strategy a secret (sometimes even from senior managers), but apart from a very few really confidential strategies, most of the strategies are, and can be, publicly known. Strategies which can be made common knowledge should be conveyed explicitly to all staff. This has many advantages as it sends the first strong message of openness and transparency within the organisation. The employees can understand their role in the organisation and feel part of it<sup>72</sup>.
  - o Purpose/ objectives of Risk Management. These generally include:
  - o Aligning risk and strategy;
  - o Enhancing risk response decisions;
  - o Improving predictability;
  - o Identifying and managing cross-enterprise risks; and
  - o Improving risk awareness and culture throughout the organisation. Make the process of improvement in the company embedded and continuous
  - o Reports that will be generated (including frequency) in the Risk Management process.
  - o Frequency of meetings that the Board of Directors (BoD) will conduct to supervise and discuss Risk Management.
- Risk Management structure. The Risk Management structure should reflect the needs and realities of the organisation. For example, the members of the internal Risk Management organisations could include dedicated employees or employees with additional responsibilities depending on the size, nature, and complexity of the enterprise. However, for big companies as covered in this study, it is recommended that there should be at least one designated Head of Risk Management. There are several examples of Risk Management organisations in the case studies presented in this study. The positions recommended in addition to the already existing Board of Directors (BoD), CEO and Executive Board (ExB) and auditing functions include:

---

72 Liker (2004: 330)

- o Head of Risk Management;
- o Risk co-ordinators;
- o Risk Owners;
- o Response Owners; and
- o Risk Champions.

The policy document is a proof of the Board of Directors (BoD) commitment and intent to the process and the whole Risk Management will be centred on the philosophy proposed by this document.

#### **c) Risk Management Guidelines/ Directives**

This document is initiated by the management of the organisation. It provides the details as to how it will set out to achieve what has been proposed by the Risk Management policy. It goes a step deeper than the policy and details the issues cited in the Risk Management policy, for example the flow of the Risk Management process, the role of the various members of the Risk Management organisation, the linkage between risk and strategy, details of reports to be generated, tools to be used, and so forth. Appendix 2 provides a real life example (anonymous) of detailed Risk Management Policy and Guideline document.

#### **d) Risk Management Handbook**

The Risk Management handbook is especially for the use of practitioners of Risk Management who have to analyse the risks and implement actions for their successful mitigation of those risks. The document provides the detailed description and methodology for various analytical and decision-making techniques to identify risks, conduct workshops, carry out qualitative and quantitative analysis, and manage information and generate reports in the Risk Management tools. This document should be able to help any employee assigned the task of managing risks, according to the guidelines and process prescribed by the management.

### 3. Risk Identification

The identification of risks is the most important and delicate step because it sets the agenda. Risks are normally only discussed when they have occurred or identified before. The worst risks are the unidentified ones, which appear suddenly and where there is no guarantee that only the Executive Board (ExB) is the first to observe them.<sup>73</sup> It could be any employee anywhere in the whole organisation who could have observed a disaster waiting to happen, but is not on the Board of Directors (BoD) and Executive Board (ExB) radar. In this step, an effort is made to identify as many risks as possible and create a Master Risk List.

Identification has to be carried out in the whole organisation to gain a complete picture of the risk landscape. A top-down and bottom-up approach should be utilised:

- Bottom-up approach helps to gain a complete picture of risks facing a company; and
- Top-down approach helps to aggregate these risks, analyse them, prioritise them, and finalise the responses and actions to overcome them.

The bottom-up approach to gather Risk Management information can be undertaken easily with the help of a simple enterprise-wide risk identification form (Appendix 5). At the end of this exercise, an aggregated/ consolidated list of risks (The Master Risk list) is ready to be classified, analysed, and prioritised. If the company is small or medium (up to 1000 employees) all the employees can be included in such an exercise. For larger companies, a cross section of 500-1000 employees per division can be involved each year in such an exercise. If this process is not considered feasible for any reasons in a company, it can be done with the help of workshops where an interdisciplinary team performs a brainstorming for the significant areas of risk in a company. A Risk Map is used displaying various risk areas.

While applying the Brainstorming technique, some rules have to be taken into consideration in order to conduct good risk identification:

- Participants: Overall view / broad perspective;
- Ambiance: Every opinion is welcome;

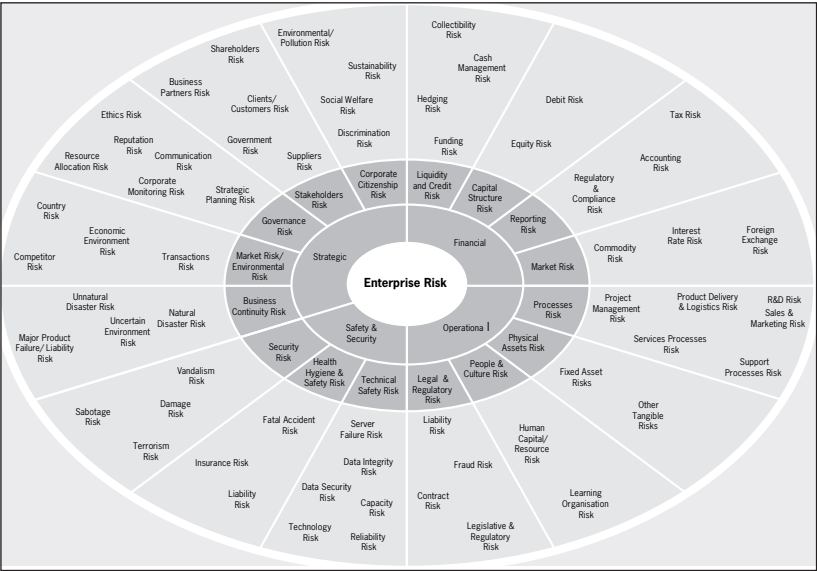
---

73 Boutellier and Kalia (2006)

- Initial position: Clarified (SWOT);
- Goals: Clarified in a balanced scorecard; and
- Moderation: Not the boss, but the risk manager.

These risks need to be classified so they can be easily assigned later on to the appropriate team of people to manage. It is good to classify risks along the lines of strategy classification as this helps to link strategic planning to Risk Management. For example, if the company is using the Balanced Scorecard (BSC) then it could classify risk into the categories of Finance, Customers, Process, and Potential. However, classification has to be based on a logic that should reflect the uniqueness of the organisation. The figure 15 below provides one such classification.

Figure 15: Risk Classification<sup>74</sup>



Source: Kalia (2006)

74 The figure has been developed with the participation of Mr. Hans von Pfullstein, research associate at the Technology and Innovation Management Institute at the Swiss Federal Institute of Technology, Zurich.

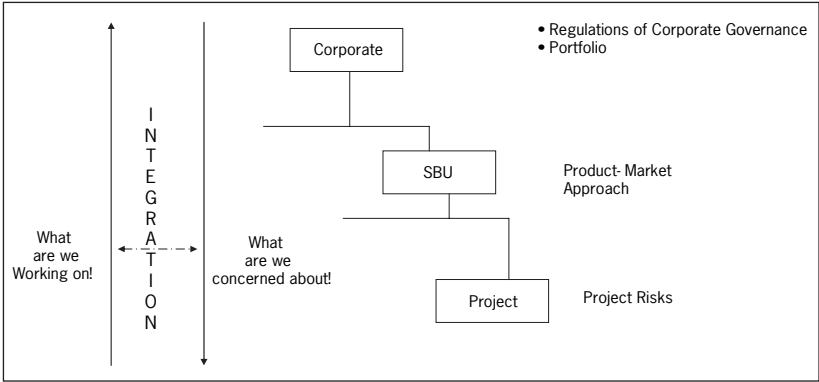
It will be important to emphasise that this is just an example. These classifications have to be thought about and implemented by the company in the most suitable way.<sup>75</sup>

**4. Risk Assessment and Prioritisation**

The Master Risk List gives a complete portfolio of risks that a company faces at a given point in time. Owing to the limited resources that any organisation possesses, it is not possible to manage all these risks effectively. Therefore, risks should be prioritised so that the company can focus only on the substantial top-level risks to be effectively mitigated. This needs assessment of the risks mapped out in the master risk list, i.e. what could be the probability of a particular risk to occur, what could be the impact, and how well is the company prepared to manage the risk if it occurs at the time of the assessment.

Failure Mode and Effects Analysis (FMEA) is one robust technique for the purpose of assessment and prioritisation. A FMEA can be carried out on different levels of the enterprise (see Figure 16). It is suited to the lowest level (products), but also to projects.

Figure 16: FMEA Works at All Levels



Source: Boutellier and Kalia (2005)

75 Definitions of all the risks classified in the above document can be found in the author's PhD dissertation (Kalia, 2006)

FMEA has a very good record in Risk Management in production, services, and technical work units. They have a strong statistical base but for practitioners it is very simple as it works on the basis of the relative positioning of risks rather than absolute numbers.

For the FMEA analysis workshops should be organised. Workshops have several advantages in that they

- Bring together people from diverse backgrounds;
- Provide a platform for «Risk Dialogue» in the company; and
- Help organise «Group Decision Making» which, if done properly (following the rules of diversity, independence, decentralisation, and aggregation mechanism) have been proven to provide optimum results exceeding even the results provided by experts.<sup>76</sup>

In the FMEA workshop, on an agreed scale (1-5 in the example provided here as it helps the easy creation of a 5x5 risk matrix of a risk-map) risks are assessed using the following criteria:

- Impact: Potential damage;
- Probability: Possibility of occurrence; and
- Surprise: Degree of preparedness if the event does occur.

The three dimensions are put into the risk FMEA spreadsheet and multiplied with each other. The product is a Risk Priority Number (RPN). A common measure for risk classification is the assignment of each particular risk to one responsible position (risk action responsible) (see Figure 17).

---

<sup>76</sup> Surowieki (2004)

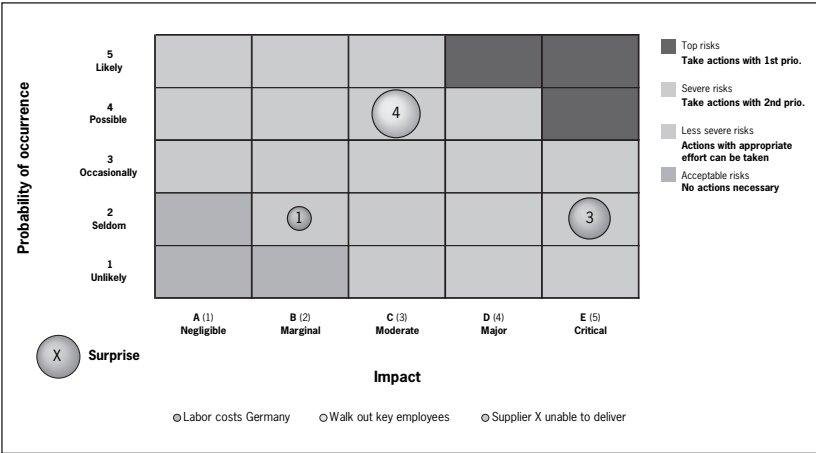
Figure 17: Risks Listed Based on FMEA Workshop

| Identification and analysis of risks |                                        |                      | Assessment of risks       |                        |                                                      | Classification of risks    |
|--------------------------------------|----------------------------------------|----------------------|---------------------------|------------------------|------------------------------------------------------|----------------------------|
| No.                                  | Risk                                   | I<br>Impact<br>[1-5] | P<br>Probability<br>[1-5] | S<br>Surprise<br>[1-5] | RPN<br>Risk Priority Number<br>$I \times P \times S$ | Risk action<br>responsible |
| 1                                    | Supplier X unable to deliver           | 5                    | 2                         | 3                      | 30                                                   | Head purchasing            |
| 2                                    | Walk out key employees                 | 3                    | 4                         | 4                      | 48                                                   | Top Management             |
| 3                                    | Labor costs Germany                    | 2                    | 2                         | 1                      | 4                                                    | Head production            |
| 4                                    |                                        |                      |                           |                        |                                                      |                            |
| 5                                    |                                        |                      |                           |                        |                                                      |                            |
| 6                                    |                                        |                      |                           |                        |                                                      |                            |
| 7                                    |                                        |                      |                           |                        |                                                      |                            |
| 8                                    | <i>List up all the possible risks</i>  |                      |                           |                        |                                                      |                            |
| 9                                    | <i>identified during brainstorming</i> |                      |                           |                        |                                                      |                            |
| 10                                   |                                        |                      |                           |                        |                                                      |                            |
| 11                                   |                                        |                      |                           |                        |                                                      |                            |
| 12                                   |                                        |                      |                           |                        |                                                      |                            |
| 13                                   |                                        |                      |                           |                        |                                                      |                            |
| 14                                   |                                        |                      |                           |                        |                                                      |                            |
| 15                                   |                                        |                      |                           |                        |                                                      |                            |
| 16                                   |                                        |                      |                           |                        |                                                      |                            |
| 17                                   |                                        |                      |                           |                        |                                                      |                            |
| 18                                   |                                        |                      |                           |                        |                                                      |                            |
| 19                                   |                                        |                      |                           |                        |                                                      |                            |
| 20                                   |                                        |                      |                           |                        |                                                      |                            |

For a company with a single source supplier the risk that a contractor does not deliver has a critical impact; it is therefore weighted with 5. In this example the probability for this event to occur is rated with a low value, 2, meaning that it seldom occurs. The event is rather foreseeable, as there will be signs indicating the supplier's difficulties before delivery stops. A low value, 2, is assigned to the surprise factor. The product of the impact, the probability and the surprise equals 20.

The same procedure is executed for all other risks. For a better visual illustration, the results are displayed in a *Risk Map* (see Figure 18). The x-axis shows the impact, the y-axis the probability of occurrence. The size of the bubble varies with the weight of the surprise factor.

Figure 18: Risk Map<sup>77</sup>



The closer a risk is situated to the top right corner of the map and the larger its size, the more severe the risk. The impact does not need to be analysed only in terms of financial considerations but could also be analysed in terms of the disruption of operations, people, and reputation.

The first and foremost thing to remember when dealing with surprise is that the only effective way to manage surprise, the third dimension of analysing risks, is to keep reserves, i.e. managing surprise requires resources. Firms have only limited resources and that makes prioritising risks very important as it provides the right focus for Risk Management. Prioritising risks helps the enterprise use few available resources at the right place. The number of risks to be strictly pursued depends on the enormity of the risks and the amount of resources that a company has. As a rule of thumb, a maximum number of 10 risks should be pursued.

<sup>77</sup> The concept has been developed at the Technology and Innovation Management Institute at the Swiss Federal Institute of Technology, Zurich.

## 5. Risk Analysis

Once the top risks have been selected based on the FMEA methodology, an in-depth analysis must follow to ascertain the main drivers of the selected risks and the appropriate measures that can be adopted to effectively manage those risks. The output of this step is the Risk Driver Tree and the Measure Map.

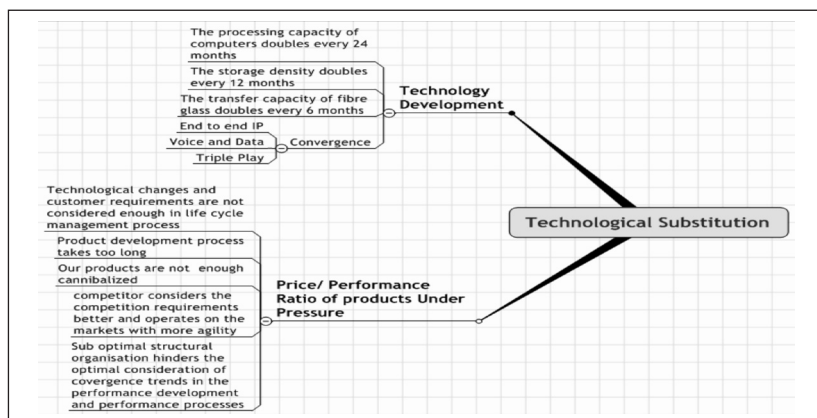
The risks are lowered by specific actions. The budget plan should integrate these actions. It needs in-depth analysis to reach conclusions regarding what actions need to be taken. The three key requirements include:

- Risk quantification;
- Identify key risk drivers; and
- Identify suitable actions to respond to the key drivers.

### a) Key Drivers Analysis/ Root Cause Analysis

Several factors contribute to a risk event. Only few of those contributing factors have a major role in the final impact.<sup>78</sup> The process of analysing these main drivers of risk is termed as key driver analysis or root cause analysis. Once the key drivers with the biggest impact are identified, it is better to act on those drivers, hence to optimise the use of the scarce resources that a company has at its disposal.

Figure 19: Example of a Key Driver/ Root-cause Analysis



78 In line with Pareto's 80:20 rule (1896 – 1897)

## **b) Suitable Actions to Respond to the Key Drivers**

Actions have to be taken to impact the biggest risk drivers. With the FMEA type workshops, most of the actions planned were based on the intuitive insights of the participating members. However, in this step, for each of these actions there has to be a detailed cost-benefit analysis, i.e. how much do these actions cost in terms of time, finance, operations and human resources, and their benefits. It is understandable that the benefits need to outweigh the costs and reduce the risks to acceptable levels. It is normally not possible to reduce the risks completely. The actions should be supplemented with milestones and Key Performance Indicators (KPI) so that their effectiveness and implementation can be observed and controlled over time. Once the actions have been planned they have to be managed by the *response owners* or a *response-owner team*. Wherever possible, teams should be assigned rather than individuals as there is a danger that the terminology at hand, such as risk-owner or response-owner or action owner, makes the people chosen responsible, thereby diluting the collective responsibility of the Executive Board (ExB) and Board of Directors (BoD).

It takes time and resources for action planning to be completed successfully. The FMEA methodology<sup>79</sup> can also be used here to move fast and include more people in this process. Once the main responses/ measures are chosen, a more in-depth analysis can be made on the chosen few measures (see Figure 20). Risk and response could have both resulted in the same abbreviation RPN, and hence the use of the word measure instead of response.

---

79 This methodology has been developed by the Risk Management team of the Technology and Innovation Institute at the Swiss Federal Institute of Technology, Zurich, Switzerland.

Figure 20: Measures Listed Based on FMEA Workshop

| Identification and analysis of measures |     |                   |                    | Assessment of measures      |                                       |                                                             |
|-----------------------------------------|-----|-------------------|--------------------|-----------------------------|---------------------------------------|-------------------------------------------------------------|
|                                         | No. | Measures          | C<br>Cost<br>[1-5] | E<br>Effectiveness<br>[1-5] | EI<br>Ease of implementation<br>[1-5] | MPN<br>Measure Priority<br>Number<br>$C \times E \times EI$ |
| Risk 1                                  | 1   | Example measure A | 2                  | 1                           | 4                                     | 8                                                           |
|                                         | 2   | Example measure B | 1                  | 4                           | 2                                     | 8                                                           |
|                                         | 3   | Example measure C | 4                  | 5                           | 3                                     | 60                                                          |
|                                         | 4   |                   |                    |                             |                                       |                                                             |
| Risk 2                                  | 5   |                   |                    |                             |                                       |                                                             |
|                                         | 6   |                   |                    |                             |                                       |                                                             |
|                                         | 7   |                   |                    |                             |                                       |                                                             |
|                                         | 8   |                   |                    |                             |                                       |                                                             |
| Risk 3                                  | 9   |                   |                    |                             |                                       |                                                             |
|                                         | 10  |                   |                    |                             |                                       |                                                             |
|                                         | 11  |                   |                    |                             |                                       |                                                             |
|                                         | 12  |                   |                    |                             |                                       |                                                             |
| Risk 4                                  | 13  |                   |                    |                             |                                       |                                                             |
|                                         | 14  |                   |                    |                             |                                       |                                                             |
|                                         | 15  |                   |                    |                             |                                       |                                                             |
|                                         | 16  |                   |                    |                             |                                       |                                                             |
|                                         | 17  |                   |                    |                             |                                       |                                                             |
|                                         | 18  |                   |                    |                             |                                       |                                                             |
|                                         | 19  |                   |                    |                             |                                       |                                                             |
|                                         | 20  |                   |                    |                             |                                       |                                                             |

The measures found, for each top risk, are assessed based on the following criteria:

- Cost;
- Efficiency; and
- Ease of implementation.

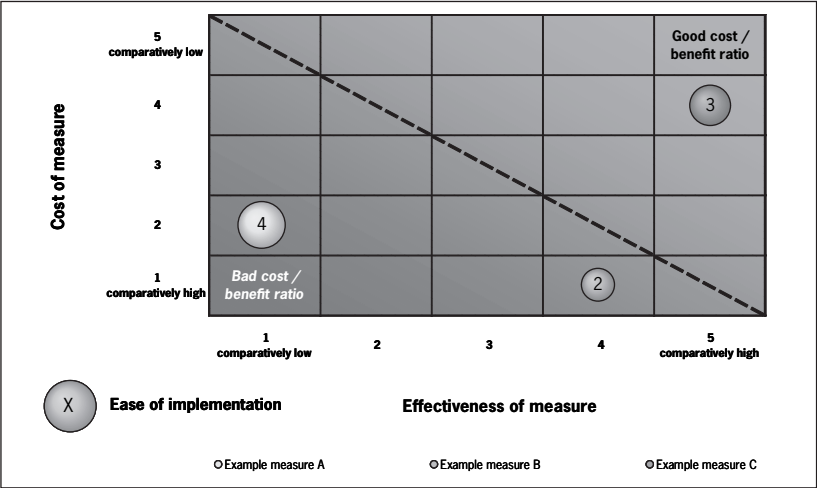
The three dimensions are put into the FMEA spreadsheet and multiplied with each other. The product is a Measure Priority Number (MPN).

The following measures, against the risk of supplier x being unable to deliver, are identified: Build up second supplier, supervision of supplier x, buy production plant. The cost of building up a second supplier is low and therefore a rather good rating, 4, is attributed. This measure will reduce the risk significantly leading to a high efficiency value. For various reasons, it is hard to implement this measure within the company; the value 2 is assigned to facilitate implementation.

This analysis is conducted for all other measures of all the risks.

The measure matrix displays the results (see Figure 21). The efficiency of a measure appears on the x-axis and the cost of a measure on the y-axis. The size of the measures displayed serves as an indicator of the ease of implementation.

Figure 21: Measure Matrix



Measures situated in the lower left corner offer a bad cost / benefit ratio, those in the upper right corner a good one. The supervision of supplier x and the acquisition of a production plant show the same cost / benefit ratio. As the first measure mentioned has a higher value of ease of implementation it is the better one.

Building up a second supplier reveals a good cost / benefit ratio, but a low value of the ease of implementation.

Either measure «supervision of supplier x» or «building up a second supplier» should be chosen for implementation.

Risk Management functions only if the risks are explicit. Therefore, in the enterprise one tries to grasp many risks in a process, to value and to fix priorities. Nonetheless, this only functions in an open enterprise culture which permits open discussions even on disagreeable and controversial topics.

## **6. In-depth Risk Analysis**

In the previous sections, the risks were identified and measures planned based on the FMEA workshop. However, once the key risks and measures have been selected based on these workshops, an in-depth analysis is carried out to ascertain reasonable financial values for those risks and the effect of the measures proposed. The difference being that workshops were based on a scale and the in-depth analysis values are based on probabilities and quantified values.

### **a) Quantification of the risks**

It is important to quantify the risks as it helps understand the scenario if the risk event really occurs. Additionally, it brings the complete risk picture into perspective. The quantified number also becomes a benchmark against which the success of actions has to be compared. The quantified number is then compared to EBITDA of the company. An EBITDA-based comparison is not the best method but it is simple for the organisation at large to understand. It is the right approach to start, but as the Risk Management function matures in an organisation a more sophisticated approach can be taken, such as comparing the risks to capital value or economic value added.

Those risks which can not be reliably quantified should be judged after a risk dialogue and an intelligent guess should be decided upon. The principle of the 70 percent solution of the US Corps should be remembered<sup>80</sup>: «Its better to decide quickly on an imperfect plan than to spend time considering every angle, and roll out a perfect plan when it's too late». The time and resources saved in this way (rather than spending lots of it on unreliable quantification) should be spent on taking actions and generating a sense of security with regard to those risks.

## **7. Action Planning**

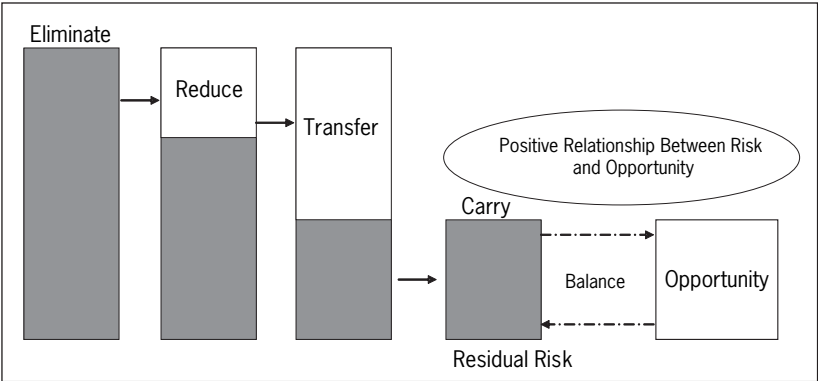
In this step, a Target Risk Map is planned representing the future Risk Map after the proposed measures are taken to mitigate the prioritised risks. The Target Risk Map also provides a benchmark against which the effectiveness of the measures can be later verified and engineered accordingly.

---

80 Freedman (2000: 8)

If one tackles risks consciously, the same four logical steps always arise to reach a balance between risks and opportunities<sup>81</sup> (see figure 22). Success strongly depends on the risk type and the risk policy of the enterprise. If the possibility to consciously form risks and opportunities exists, it makes little sense to enter into risks without being able to realise opportunities. It is advisable to remember that the model presented in figure (22) holds true for only the known risks. However, as hard as one might try, there will always be some risks that will surprise us as they are not identified by the identification process. That is the reason for focusing on surprise and its management through strategic reserves.

Figure 22: Risks Gradually Reduce

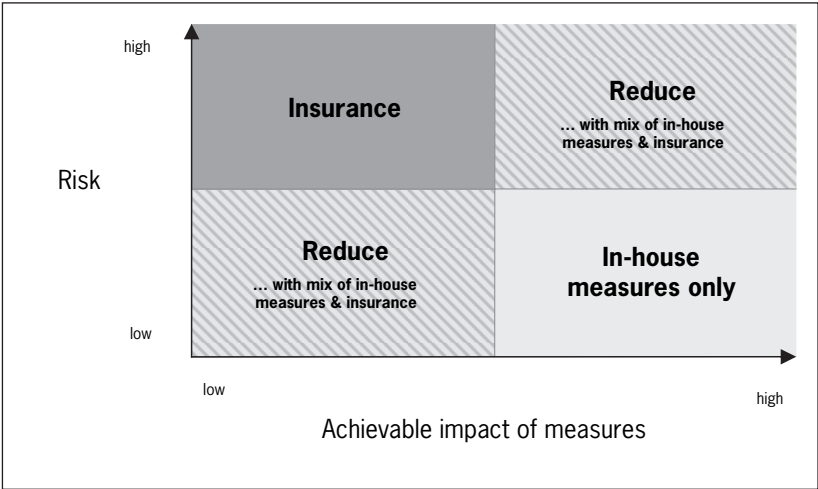


Source: Boutellier and Kalia (2006)

The actions planned have different capacities to achieve results. An appropriate strategy should be utilised as shown in the figure (23).

81 Boutellier, R. and Kalia, V. (2006)

Figure 23: Key Strategies to Manage Risks<sup>82</sup>



### 8. Monitoring, Reporting and Supervision

In order to implement measures as described in the previous sections, and that the organisation learns consciously, monitoring and supervising/controlling actions is necessary. The purpose is to compare the actual Risk Map (after the measure has been implemented) to the target Risk Map and check the effectiveness of the measures adopted (and change some if they have been ineffective).

Regular reports have to be generated for the purpose of providing the complete picture of the risk at that time. It is advisable to have a quarterly reporting structure. Controlling should take place not only on the level of single actions, but also on the level of the whole process. Companies must integrate actions into the normal report process according to importance, and actions can then be pursued in detail or as individual projects.<sup>83</sup> The Risk Manage-

82 The concept has been developed with the participation of Prof. Dr. R. Boutellier, Mr. Vinay Kalia and Mr. von Pfullstein at the Technology and Innovation Management Institute at the Swiss Federal Institute of Technology, Zurich.

83 Boutellier and Kalia (2006)

ment process should be checked periodically at least every two to three years as a whole. The reports should be kept as simple as possible. For the Board members a summarised report (not more than 2 pages) showing all risks, major actions, action owners and key milestones achieved and being pursued should be presented. However, the Board of Directors (BoD) should be able to receive any amount of in-depth information as they want on the basis of which these reports are made. A typical risk report must cover the following:

- The present status of the risk;
- The previous status of the risk;
- Movement of the risk (increase / decrease);
- A comparison of the performance of action implementation and its effectiveness against the established Key Performance Indicators (KPI);
- Special comments;
- New risks on the radar or unexpected events; and
- Comment on quality of Risk Management.

Another important ingredient of risk reporting includes a time-series analysis of risk. The benefit of this analysis is that it provides a good understanding about the way risks are developing, i.e. whether they are reducing or increasing, and whether the risk response strategies are successful or not. Many new risks recur and disappear from the Risk Map as this analysis clearly shows the movement of the risks. Time-series analysis provides an opportunity to shift the discussion from absolute numbers through quantification (generally based on unreliable data) to trends the risks are following, for example, if an IT server risk is on the radar. It will slowly start to disappear from the risk matrix as a back-up server is installed.

However, to conduct the time-series analysis, the Risk Management process should have been established in the organisation for some time. Normally, a year after the action implementation is a good time to start time-series analysis.

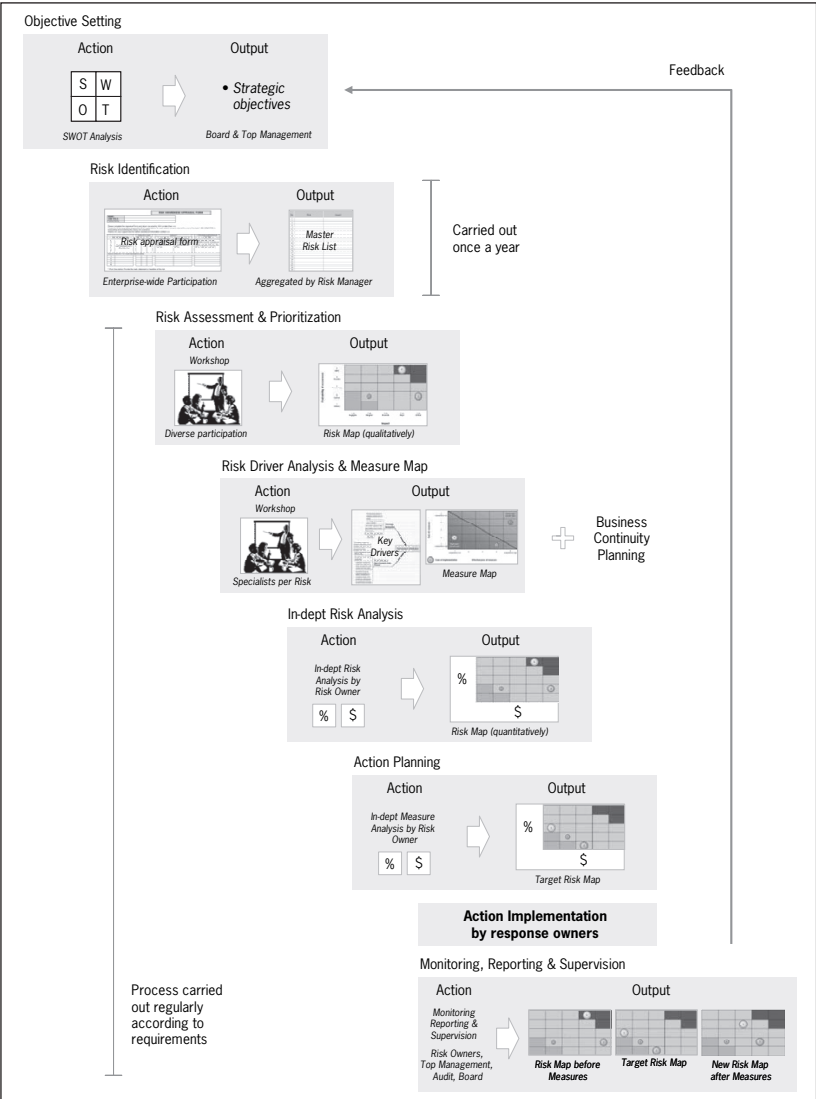
Once every year, a comment on quality of Risk Management has to come from two sources:

- Internal control and audit; and
- Head of Risk Management.

The internal control and audit report focuses on implementation aspects, i.e. whether the actions have been performed as suggested by the key performance indicators, whether the milestones have been achieved according to the deadlines, and whether the process has been followed diligently and according to the stated policies and guidelines.

The Head of Risk Management in consultation with other members in the organisation provides a report on whether the actions taken were good, how they benchmark with the other companies and what could be done to further improve analysis and actions in the next cycle of Risk Management. The help from outside experts is also suggested. Figure (24) provides an overview of the Enterprise Risk Management Implementation process as discussed in this section.

Figure 24: ERM Implementation Overview<sup>84</sup>



84 The figure has been developed with the participation of Mr. Vinay Kalia and Mr. Hans von Pfuhlstein from the Institute for Technology and Innovation Management, ETH Zurich.

## 9. Culture

It is not only a problem to implement Enterprise Risk Management in a company with global operations but also in group companies with various divisions and businesses based only in one country, as bridging existing cultural differences is difficult. It is not surprising that «culture» is termed one of the most important aspects in implementing Risk Management by the members of Boards of Directors (BoD) and top managers.

Risk Management is currently a priority at senior organisational levels, rather than throughout the organisation. The issue of being successful in establishing Risk Management culture is difficult. Only 15 percent of companies, according to one survey<sup>85</sup>, feel that they are successful in that endeavour. The most common methods employed for developing such a culture are:

- Publicising Risk Management guidelines for all employees;
- Developing a Risk Management handbook (or something equivalent) in which detailed information regarding corporate Risk Management processes and tools is provided;
- Defining risk champions in various parts of the organisation; and
- Highlighting the importance of Risk Management in the Annual report and other internal communications such as company newsletters.

In addition to the points mentioned above, there are several creative ways in which companies spread Risk Management culture. The success of Risk Management has to be «marketed» in the organisation. The more people can relate and observe success, the more they are inclined to accept Risk Management and find it less of a bureaucratic exercise. Tangible benefits should be demonstrated to management and employees. If the risks are quantified, it is easy to demonstrate the tangible benefits as this can clearly show the potential impact of an event with, or without, the Risk Management intervention. However, there are few risks that can be reasonably quantified. For those situations, success can be interpreted in the following ways:

---

85 Conducted by Transfer Center for Technology Management (TECTEM) at the University of St. Gallen, Switzerland.

*External perception:* It is important to see how the external observers analyse and rank the company. For example, if insurance premiums are stable it means that insurance companies have trust in the Risk Management success of the company and is assured against the company's failures. Similarly, if share prices perform well, this will reflect the confidence of shareholders in the company that it is likely to achieve its stated objectives and is hence undertaking good Risk Management.

*Analysing losses:* Companies could create a data bank of losses occurring due to negative events before, and after, the initiation of Risk Management. The consistent reduction of losses should demonstrate the success of Risk Management initiatives.

*Meeting the objectives laid out:* Risk Management is about consistently making choices and then later on checking if the choices were right. This enhances the process of the organisational learning curve. The laying out of objectives to be met in a certain timeframe should be set and then evaluated at the end of the time planned. If objectives are met, this can be interpreted as success. However, provisions should also be made to evaluate unforeseen risks and how the Risk Management set-up coped with those risks.

*A periodic evaluation from the various stakeholders:* The rise or fall in the perceived confidence of the various stakeholders, i.e. analysts, employees, Board members, Executive Board (ExB) and more. The level of perception will determine the success or failure of the Risk Management set-up in the organisation.

*Level of awareness in the organisation:* A high level of awareness regarding Risk Management in the enterprise, i.e. across hierarchies and across functions, will signify not only that Risk Management is being successfully carried out, but also that the organisation has been successful in spreading the Risk Management culture. This awareness can even be analysed over informal meetings. Answers to a simple question such as «What are the three biggest risks being faced by the organisation?» will tell a lot about the culture, transparency, and success of the Risk Management function in the company.

## 10. Tools

There are two main requirements for which IT tools are needed:

- The ability to aggregate risk-related information from across the organisation, such as risks identified, responses implemented, reports generated, and the status of the various milestones to be achieved in managing risks; and
- The ability to quantify these risks and run statistical analysis such as correlation analysis, Monte-Carlo simulations for calculating the Value-at-Risk (VaR) and Time series analysis for studying the movement of a risk over a specific period of time to check if it is increasing or decreasing.

In most cases, these tools have been established by companies themselves with assistance from consulting firms and software providers. Such effort have the advantage that self-developed tools are tailored to the company's requirements, whereas standard tools could hinder (or inadequately aid) the company.

Whereas it appears that there is a market for an IT tool that can integrate these two requirements, no such tool is currently available. Companies have advanced from using relatively simple aggregation systems (Excel, access and word based systems) to more customised and sophisticated systems. This is especially true for information aggregation systems. Quantitative tools are still not as well-developed as some users might want them to be. The difficulty lies in the fact that most of the tools are based on statistics and probability, thus predisposing them to application in contexts in which data are available in a form that can be used to generate robust and trustworthy results. This is more likely to be the case in financial and trading contexts.