PUBLISHED BY
bookboon

Olaf Passenheim

Enterprise Risk Management

Prof. Dr. Olaf Passenheim

Enterprise Risk Management

Enterprise Risk Management
1st edition

ISBN 978-87-7681-684-1

Contents

List of Figures

1 Introduction

1.1 Risks are Opportunities

Earlier, so it seems, the world was less dangerous. Today, more and more enterprises with innovative, complicated technologies and sensitive know-how work at an international level. The greater, the stage becomes on which they move and the more complicated the role they play, the more numerous become the traps which potentially endanger the achievement of the enterprise's aims. Hence, raised attention and suitable instruments to play this game are – especially in a difficult economic sphere – more than ever compulsory.

Today new technologies are under the magnifying glass to a much greater extent that previously. There might be two reasons for this. Firstly, nowadays, most economic disasters are published worldwide within seconds and become known in an instant. Secondly, many new technologies are considered to be risky: James Watt in his time produced steam boilers with one rather low overpressure risk. A malfunction with one of his machines would have had an effect of only some meters and would have been limited to a short time span. However, "modern" catastrophes like Chernobyl had an effect of some thousand kilometers and the resultant radioactivity may still be problematic for many generations to come.

The combination of fast communication and a wider spread of the effects of errors are responsible for the call for risk management at an enterprise level. Company scandals like those at Enron, Swissair and AIM have devastated the stock market and diminished the overall value of stocks by several billion dollars. Trust in the controlling ability of the auditors with regard to stock market supervision has been lost. Pension funds, the big financiers of the 21st century, require transparency in the form of a professional evaluation of the business risks and an open communication of the most important dangers which a business might face.

Complex markets, an advancing regulation density and rising requirements for the transparency and effectiveness of companies are only few of various business risks. Questions by the shareholders or the board of directors regarding the actual risk situation of the company often result in the need for comprehensive auditing of the actual risk situation.

1.2 Risk Management vs. Enterprise Risk Management

As a consequence of economic crisis many executives now recognize that single risks can be valued realistically only in their interaction with other risks. Risks should no longer be regarded isolated, but be identified, analyzed and controlled within the framework of all interacting risks. As recent studies confirmed, almost every company looks at these risks in isolation. During the past years, separate subsystems have developed in many companies, for example, on account of legal requirements for the management of risk. These companies look at single risk ranges, for example Treasury or Compliance. The dependence between the risks often remains unnoticed.

The management of risk up to now places the main focus on avoiding the repetition of errors made in the past. The fact that basic conditions can quickly change, like competitive environments or raw materials prices, are often out of sight. Structures for the risk management in a company as well as models and methods for risk management which are based on established, statistical and technical experiences do not always consider the constant changes in the market environment and in the company structure. What is often missing is a logical alignment of risk management with strategic business goals (see figure 1).

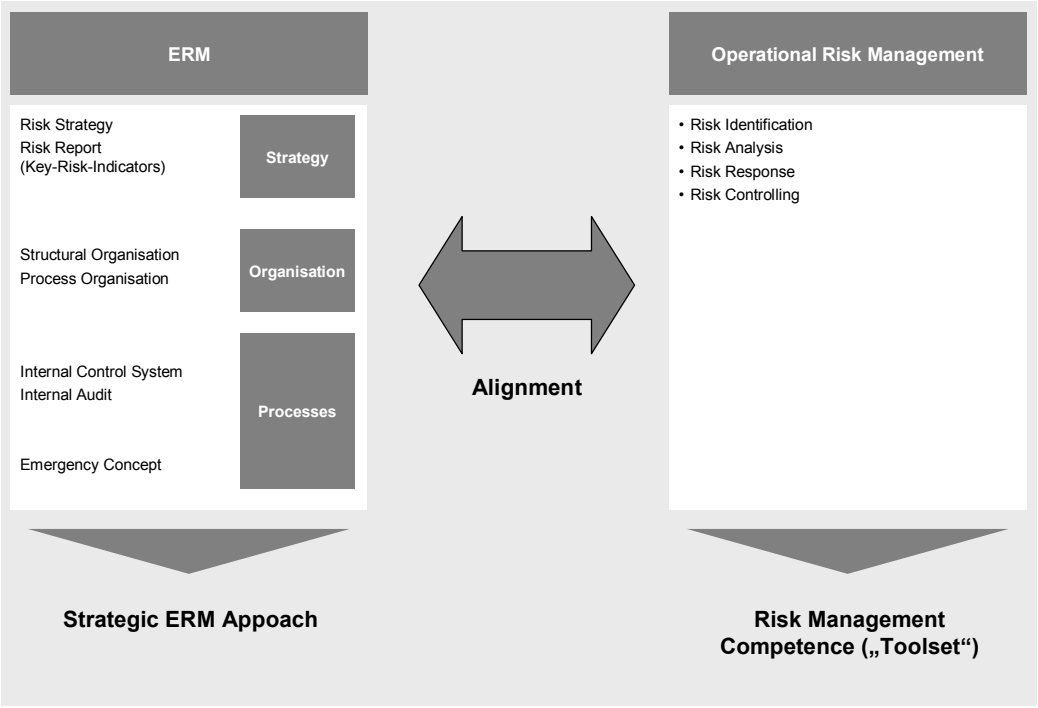

Figure 1: Missing alignment of ERM and operational Risk Management

The challenge for a company is to bring together its established subsystems with the goal to develop an integrated, company-wide risk management system with dynamic structures. To make the risk management function, it must orientate itself not only to the goals of the company, but also to its strategy and culture. The goal a company wants to achieve with its risk management strategy must be compatible with the overall business objectives. Parallel, lessons learnt from risk management can also lead to an adaptation of the business' objectives and corporate strategy (see figure 2).

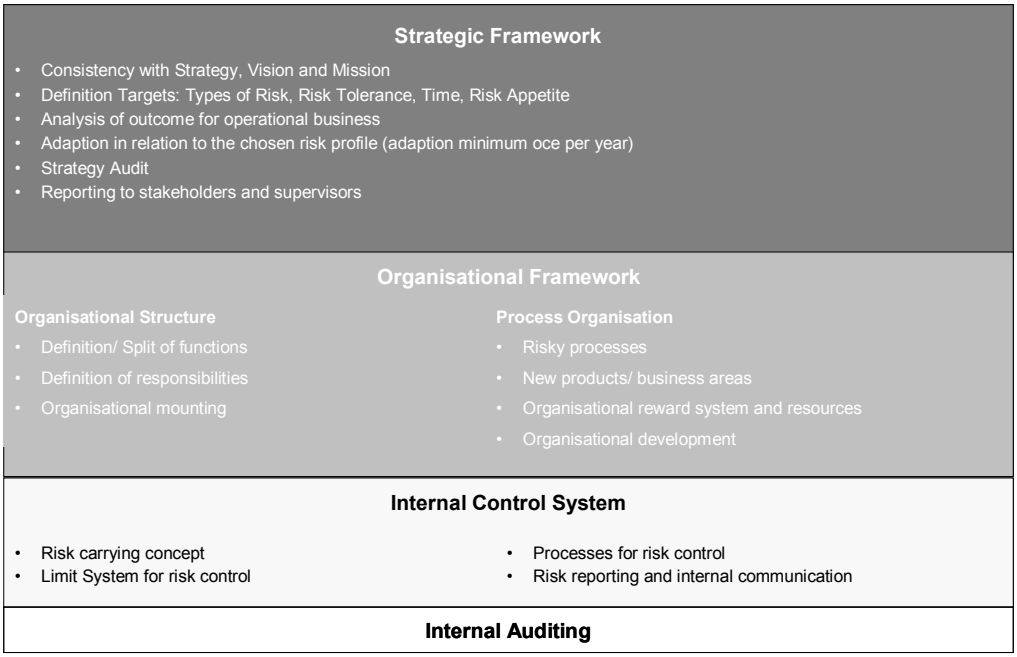

Figure 2: Integrated enterprise risk management

The industry in which a company acts and the business model are other factors of influence for a company-wide risk management model. For a company in the chemical industry, for example, environment protection orders have a high value. In the insurance industry the minimum requirements influence risk management (MaRisk VA) as the risk management must be followed and are monitored.

Finally, companies must look at the complete risk sphere in which they move. Beside the classical risks which can be strategic, financial and operational nature or concern the legal environment, so-called emerging risks must be also considered. Emerging risks are global risks which can be predicted only hard, for example climate change, political instability or volatile energy prices.

1.3 Framework of ERM

There is not yet an internationally binding framework for enterprise risk management. Even terms like "Corporate Governance", which seems to be understood in the same way by most companies, have no binding legal background in most cases but are more a declaration of will towards the share- and the stakeholder. Nevertheless, there are some frameworks which can be used as a platform to get enterprise risk management started:

- ISO 31000
- Sarbanes Oxley Act
- Corporate Governance Codex
- COSO and COSO II

1.3.1 ISO 31000

Since end of 2008 there is a valid worldwide standard on the subject risk management: The international norm is ISO DIN 31000. Together with the revised ISO guide IEC 73 "Vocabulary", this norm was published at the end of 2009.

In the new ISO 31000 three principles are anchored: Firstly, risk management is understood to be an executive function. Secondly it is tried in the norm to move a so-called top-down estimate and thirdly, the ISO 31000 shows a very generally held base which tries to consider all the different risks within an organisation.

The ISO 31000 came, like the quality management norm ISO 9001, via general recommendations to allow a wide applicability. Paralleling this, three guides were published for the successful application of the ISO 31000:

- Embedding of risk management in the management system
- Methods of risk assessment
- Emergency management, crisis management and continuity management

Risk management sees the ISO 31000 as an executive function. The complete risk management system is based on the principle of the PDCA cycle (Plan-Do-Check-Act): The first step, "plan", contains the risk politics of the organisation, order and liability. The second step, "Do", contains the real risk management process consisting of the execution of risk identification – risk analysis – risk valuation – risk handling. Afterwards the ISO 31000 recommends in the third step, "Check", to check the adapted risk coping strategies and with ascertained deviations from the plan in the fourth step, "Act", to remove them.

While up till now only very specific risk management norms have existed, for example, the ISO 27005 in the area of Information Security Management (ISMS), the ISO 31000 tries with a comprehensive top-down approach to register all risks and their handling within an organisation. This means a risk management after ISO 31000 is not only to be settled exclusively on a strategic enterprise level, but it also deals with the risks to operational management levels within the company.

1.3.2 Sarbanes Oxley Act

The Sarbanes Oxley Act is a regulation which passed the US Congress in 2002 as a reaction to different financial scandals. It serves primarily to recover the trust of investors in the general capital market and applies rules and standards by which company functions in order to raise the level of transparency between their financial reporting and the markets.

The Sarbanes Oxley Act is directed equally at the executive boards of companies and chartered accountants. After major financial scandals, criticism arose as well regarding the information policy as lacking responsibility for the behavior of managers. As a counteraction, regulations and reinforced controls should be realized. The financial scandals of the US companies, Enron and Worldcom, initiated this course of action.

The energy group, Enron, ranked within the top 7 US companies up until its breakdown in 2001. In 1996 its stock exchange value 50 billion US $. Its main business was commodities trading as well as the distribution of futures contracts on gas. For years the group reported profits until in the third quarter in 2001 a loss of more than 600 million US $ was suddenly announced. Moreover, a retrospective correction of the trading results for the last four years of about 580 US $ was reported. Afterwards it turned out that the information policy and dubious balance sheet transactions on the public record had clouded the exact financial situation of the company.

Charges were also raised against the chartered accountants who did not understand or reveal the situation in time so that investors were completely surprised by the sudden corrections.

The Sarbanes Oxley Act should lessen the level of influence of investors and ascribe new duties and regulations for a company, their corporate governance and their chartered accountants to enable preventive actions to take place.

Sarbanes-Oxley contains 11 titles that describe specific mandates and requirements for financial reporting. Each title consists of several sections, which are:

1. Public Company Accounting Oversight Board (PCAOB)
2. Auditor Independence
3. Corporate Responsibility
4. Enhanced Financial Disclosures
5. Analyst Conflicts of Interest
6. Commission Resources and Authority
7. Studies and Reports
8. Corporate and Criminal Fraud Accountability
9. White Collar Crime Penalty Enhancement
10. Corporate Tax Returns
11. Corporate Fraud Accountability

Critics of the Sarbanes Oxley Act argue that the act is merely a combination of already existing regulations which bring about obstacles for small and medium enterprises in achieving their IPO.

1.3.3 Corporate Governance Codex

Corporate Governance can be understood basically as the company's rules of management and control. Corporate Governance provides a juridical and general framework, in particular with regard to the integration of the company in its environment and differs in that aspect from the company constitution which deals primarily with the internal regulation of a company.

Up till now still, no uniform understanding or uniform definition of what Corporate Governance means exists. However, in general Corporate Governance can be understood as the totality of all international and national rules, instructions, values and principles which are valid for a company to determine how these are managed and monitored. In the literature one can regularly read discussions about good Corporate Governance or the improvement of existing Corporate Governance.

- Functioning business management
- Safeguarding the interests of different groups (e.g., of the Stakeholder)
- Target-oriented cooperation of the company's management and control
- Transparency in company communication
- Adequate handling of risks
- Management decisions are targeted to be long-term and value added.

The guidelines of the OECD regarding Corporate Governance are less comprehensive as a recommendation – no obligation – towards a common and least standards of a TQM or the EFQM model because only the rights of stakeholders as established by law are considered.

1.3.4 COSO and COSO II

The original COSO model goes back to the year 1992 and is more focused upon the work of chartered accountants. COSO stands for the Committee of Sponsoring Organizations and its members are recruited from the Institute of Internal Auditors (IIA), American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the American Accounting Association and the Institute of Management Accountants (IMA).

COSO supports, within the scope of the internal monitoring system, optimization of internal checks and alignment towards the company's goals. The basic idea of COSO is the combination of tasks and components of an internal control system. Components of the internal control system are operations, financial reporting and compliance.

COSO II in 2004 was expanded to include the area of Enterprise Risk Management. The basic assumption of ERM is that every organisation creates values for specific interest groups. At the same time, all organizations and management should consider it their task to determine the level of insecurity they are prepared to accept.

COSO II describes eight interrelated but different components of enterprise risk management which are: (for further detailing go to www.coso.org):

- Internal Environment – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- Objective Setting – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
- Event Identification – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channelled back to management's strategy or objective-setting processes.
- Risk Assessment – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- Risk Response – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
- Control Activities – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- Information and Communication – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
- Monitoring – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another.

The COSO II approach to the ERM shows a supplement of the classical estimate COSO of the internal control system. The main focus is on the area of general, company-wide risk management and therefore puts a spotlight on the strategic approach. Not only are risks considered, but also opportunities. This approach can be used to extend the internal control system of a company and to develop a more comprehensive risk management system.

2 Enterprise Risk Management

2.1 Events – Risks and Opportunities

Events can have negative impact, positive impact, or both. Events with a negative impact represent risks, which can prevent value adding or erode existing value. Events with positive impact may offset negative impacts or represent opportunities. Opportunities are the possibility that an event will occur and positively affect the achievement of objectives, supporting value creation or preservation. Management channels opportunities back to its strategy or objective-setting processes, formulating plans to seize these opportunities.

To understanding this, everyone can ask himself or herself the question:

What is a risk?

This simple question already shows that the definition of risk can be rather difficult as expectations are focused into the future and therefore not make sufficient allowance for uncertainties. Additionally, these uncertainties could end in an outcome that is either more positive or more negative than expected. So it might be better to start with a definition of uncertainties:

Uncertainties = Threats + Opportunities

- Threats are events that have a negative impact on any result.
- Opportunities are events that have a positive impact on results; and
- Uncertainties encompass the complete range of positive and negative impacts;

Literature often describes risk as "the possibility of suffering harm, loss or danger." Although one is usually not familiar with that definition, one has an instinctive sense of risk. Everybody is confronted with risks in taking part in day-to-day activities. For example, we could be seriously injured in the case of a car accident if our seat-belt is not fastened. If one is smoking too many cigarettes, the possibility of dying of cancer is much greater than for a non-smoker. It is not in our nature to think about all the possible risks that may affect us but risks definitely shape our behaviors. If we want to cross the street, parents have told us to always look both ways before placing one foot onto the street.

Also, in every project there is the possibility of threats and benefits which may affect the success and completion of a project. In our common understanding we associate a risk with being a problem but this is not correct. A risk is not a problem until it actually occurs. It is more a recognition that a possible problem might occur in the future.

2.2 Definition of Enterprise Risk Management

Enterprise risk management deals with risks and opportunities affecting value creation or preservation, defined as follows by the COSO:

> *Enterprise Risk Management (ERM) is a process, affected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*

However, this definition is lacking in two major aspects: Firstly, successful ERM has to be driven and carried by the whole organisation, especially the middle management and secondly, every company that uses ERM has to ensure that a "risk awareness culture" is trained, lived and rewarded within the company.

Nevertheless, the above definition reflects certain fundamental ideas. Enterprise risk management is:

- NOT part of the vision of a company, but nevertheless should be reflected in the mission statement (corporate culture)
- Applied in strategic sessions

- Applied across the enterprise, at every level and unit, and includes taking an entity level portfolio view of risk
- Able to provide reasonable assurance to an entity's management and board of directors without releasing them from their responsibility
- Objectives are set in one or more separate but overlapping categories

This definition is purposefully broad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries, and sectors. It focuses directly on achievement of objectives established by a particular entity and provides a foundation for defining enterprise risk management effectiveness.

2.3 The ERM framework

Within the context of an aligned company's mission or vision, management establishes strategic objectives, selects strategy, and sets aligned objectives cascading through the enterprise. This enterprise risk management framework can be set into four categories:

- **Strategic** – high-level goals, aligned with and supporting its mission
- **Operational** – effective and efficient use of its resources
- **Financial/Reporting** – reliability of reporting
- **Hazard/Compliance** – individual errors and compliance with applicable laws and regulations.

This categorization of entity objectives allows a focus on separate aspects of enterprise risk management.

Strategic Risks include risks from:

- Damage to reputation
- Competition
- Customer Wants
- Demographic and social/cultural trends
- Technological innovations/patents
- Capital investment, shareholder requirements and
- Regulatory and political trends

Operational Risks include risks from:

- Business operations (e.g., human resources, product development, capacity, efficiency, product/service failure, channel management, supply chain management, business cycles)
- Empowerment (leadership, change willingness)
- IT

Financial/Reporting Risks include risks from:

- Price (e.g., asset value, interest rate, foreign exchange)
- Liquidity (cash flow, call risk, opportunity cost)
- Credit (e.g. rating)
- Inflation, purchasing power and
- Basis financial risk (e.g., hedging)
- Wrong or incomplete reporting (e.g., financial performance)
- Information/ business reporting (e.g. budgeting and planning, accounting, information, taxation)

Hazard/Compliance Risks include risks from:

- Fire and property damage
- Windstorms and other natural phenomena
- Theft and other crime incl. personal injury
- Business interruption and
- Liability claims

The categories are distinct, but also overlapping. A particular objective can address different entity needs and may be the direct responsibility of different managers. This categorization also allows distinctions between what can be expected from each category of objectives. Another category – safeguarding of resources, used by some entities, also is described.

Because objectives relating to reliability of reporting and compliance with laws and regulations are within the entity's control, enterprise risk management can be expected to provide reasonable assurance of achieving those objectives. Achievement of strategic objectives and operational objectives, however, is subject to external events not always within the entity's control. Accordingly, for these objectives, enterprise risk management can provide reasonable assurance that management, and the board in its oversight role, are made aware, in a timely manner, of the extent to which the entity is moving toward achievement of the objectives.

2.4 The ERM process

Enterprise risk management is a procedure to minimize the adverse effect of a possible financial loss by

1) Identifying potential sources of loss;
2) Measuring the financial consequences of a loss occurring and
3) Using controls to minimize actual losses or their financial consequences.

The purpose of monitoring all risks is to increase the value of each single activity within the company. The potential benefits and threats of all factors connected with these activities have to be ordered and documented. If all employees are aware of the importance of the risk management process, the probability of success will be increased while at the same time failure will become unlikely.

Risk identification is not solely done by an individual. All relevant stakeholders are involved to keep an eye on all risks that matter. Generally the risk identification sessions should include as many as the following participants:

- Risk management team
- Subject matter experts from other parts of the company
- Customers and end-user
- Other project managers and stakeholders
- Outside experts
- Project team

The participants may vary but the risk management team should always be involved because they are dealing with the subject every day and therefore need fresh information at any time. Outside stakeholders and experts could provide objective and unbiased information for the risk identification step and are therefore an essential part of the process.

Risk identification has to be done as a continuous process. If it is treated like a one-time event, then the whole company runs the risk of overlooking new emerging problems. The process starts in the initiation phase where first risks are identified. In the planning stage the team determines risks and mitigation measures and documents them. In following stages of resource allocation, scheduling and budgeting the associated reserve planning is also documented.

After the initial phase of risk identification, all risks have to be managed until each risk is closed or terminated. New risks will occur as the company moves on and matures and the outer and inner environment of the company changes. In the case of the increased probability of a risk or if the risk becomes real, it is time for the risk management team to respond to it. The executives and managers have to think about the problem and develop strategies to deal with its impact. All the re-planning actions can mean a change to the baseline of budget, schedule and resource planning.

How the company will deal with risks has to be clearly defined in the early stages of getting involved in ERM, then documented and executed appropriately during the planning cycle. Figure 3 illustrates the risk management process.

Figure 3: Risk Management Process

2.4.1 Risk Identification

Risk identification is the first and most important step because it builds the foundation for all subsequent steps. The risk identification step is very similar to a transformation process. In the beginning you have inputs and in the end you have a result or simply an output. In the middle step there are tools and techniques to fulfill the transformation process as shown in figure 4.

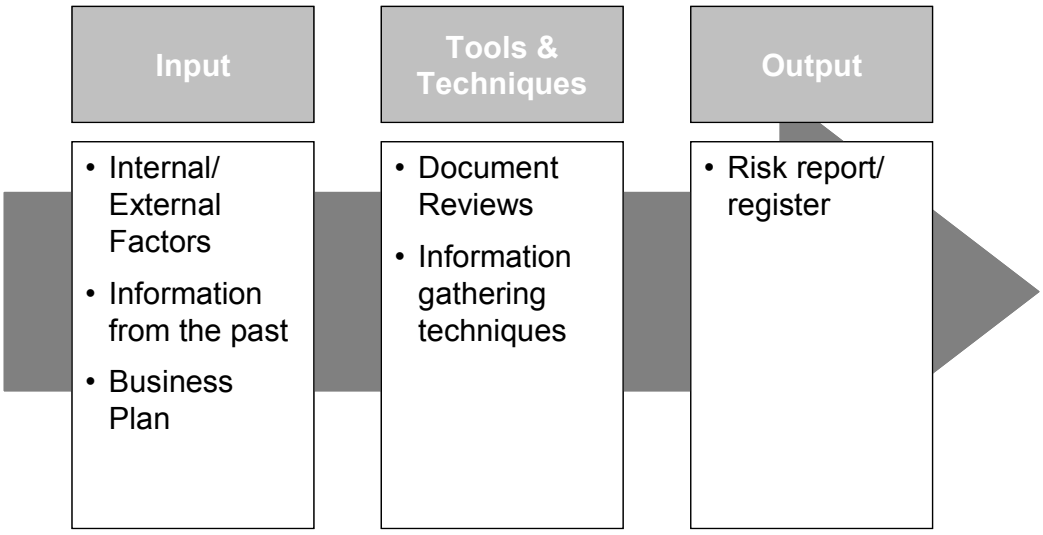

Figure 4: Risk Identification

With the first input for risk identification, external and internal factors of the project environment have to be considered. External factors could be described as the attributes of the environment whereas internal factors are attributes of the (project) organization itself. Typical examples for external factors are:

- Economic conditions
- Social, legal or regulatory trends
- Political climate
- Competition – international or domestic
- Fluctuation in demand
- Criminal or terrorist activities

Typical examples for internal factors are:

- Internal culture
- Staff capabilities/ numbers
- Capacity
- Systems and technology
- Procedures and processes
- Communication effectiveness
- Leadership effectiveness
- Risk appetite

Information from prior ERM-projects are usually records about experience, developments, hints, failures and risks which are now useful in identifying risks. The end documentation of recent projects ("lessons learnt") is a first step for gathering structured information in project management. If kept in an (electronic) archive it is very useful for the preparation of future projects.

The risk identification step requires that every relevant stakeholder has a complete understanding about the purpose of ERM. Only then will you be able to screen the task from different perspectives and to identify risks you wouldn't otherwise have identified.

Within the tools & techniques step you start with the documentation review to analyze information that already exists in a written form. This is usually the business plan and supporting documents like market- or socio-democratic information (figure 5).

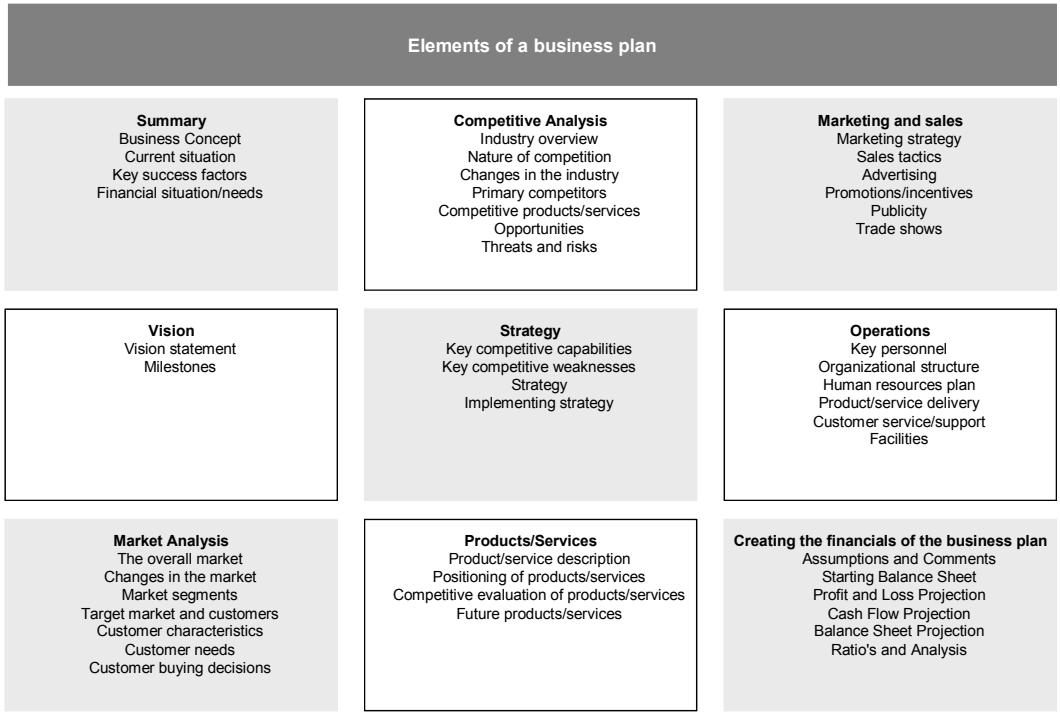

Figure 5: Elements of a business plan

By utilizing several techniques one should obtain an answer to the question, "is the business plan truly realistic in terms of budget, scope and schedule?"

Several information-gathering methods can be utilized to identify risks related to the project. The major three used are:

- **Brainstorming** – a general information-gathering and creativity technique which helps to identify risks and possible solutions for them. In a brainstorming session a group of team members and subject matter experts "brainstorm" about possible outcomes and sources of risk. Ideas are generated under the leadership of a facilitator. The brainstorming meeting should be done without interruption and judgment or criticisms of ideas. Very often the ideas of one are built upon by another. In the end each identified risk will be categorized and its description will be sharpened. The goal of brainstorming is to obtain a comprehensive list of risks.
- The **risk breakdown structure** displays an organized description of any known risks, arranged by a number of categories and their characteristics in vertical branches. Usually it will show all of the risks and their possible causes.

Enterprise Risk Management

The SWOT analysis is also used to define possible risks. In the 1960s and 1970s, Albert Humphrey conducted a research project at the Stanford University using data from 500 U.S. public corporations. From this he developed the SWOT analysis. SWOT (an acronym) looks for Strengths, Weaknesses, Opportunities and Threats. Often SWOT is used as a basis for brainstorming. By defining strengths and opportunities, ideas of known or predictable weaknesses and threats will come to mind. SWOT can be used for companies, its departments and divisions as well as for individuals. An advantage of SWOT analysis is that it is simple and relatively cheap except for the time needed to conduct it. It helps generate new ideas. On the other hand, the advantage is also the disadvantage as the ease with which a SWOT analysis is conducted means that there is no detailed information about how to reach an objective or how important a threat might be. A careful use of the outcome of the SWOT analysis is therefore highly recommended.

These tools and techniques help management to gather relevant information and in the analysis and identification of risks and opportunities for the company to achieve its aim for the project, its scope, cost and budget. The information will then be stated on the so called risk report/register, which is the main output of the risk identification step.

The risk report/register includes all identified risks and their description, risk categories, their causes, the probability of an occurrence, the single impacts of certain risks, possible responses, and their root causes. The whole risk identification process has four main entries on the risk register:

- Lists of identified risks – Identified risks with their root causes and risk assumptions are listed
- List of potential responses – Potential responses identified here will serve as inputs to the risk response planning process
- Root causes of risk – Root causes of risk are fundamental conditions which cause the identified risk
- Updated risk categories – The process of identifying risks can lead to new risk categories being added

As learnt from the previous points of risk identification, this step can comprise checklists of possible risks, surveys, meetings and brainstorming, reviews of plans, different analyses and so on. To do this correctly requires a detailed knowledge of the organization, the market in which it operates, the legal, social, political and cultural environment in which it operates, as well as the development of a clear understanding of the strategic and operational objectives of the organization, including factors critical to its success and the threats and opportunities related to the achievement of these objectives.

Risk identification should be done in a methodical way. This has to be done to ensure that all important activities and possible consequences related to those activities are identified. It is also possible to outsource the whole risk management process, but an in-house approach is usually more effective when some conditions are fulfilled. First, the communication channels should be well defined and consistent and processes and tools should be well co-ordinated.

2.4.2 Risk Analysis

The basis of risk analysis is the earlier explained risk identification. Risk analysis covers a complete and continuous evaluation which should be realized quantitatively as well as qualitatively for all identified risks. The goal is to detect possible interrelations and enable the management to identify an order of importance, also called prioritizing. Furthermore, the consequences for the company itself and its organizational goals can be identified. The evaluation of risks should meet the following demands:

- **Objectivity**: Reference to the special market should be taken into consideration in order to make the objectivity practicable. Especially risks attached to the market price of products or stocks can be detected easily. For internal risks a subject evaluation is often necessary.
- **Comparability**: The evaluation of risks should lead to comparable results. Therefore the organization should use consistent and standardized methods and data.
- **Quantification**: By means of quantification the organization is able to detect and deviation from the targeted goal.
- **Consideration of interdependencies**: In practice this is the hardest part of risk assessment.

Effects like compensation and interdependencies can emerge. Not realizing connections between risks and their meaning for the department and/or for the whole organization can be a big risk. That is why management should consider carefully what a risk and the reaction to it can mean for the whole organization as a good solution for one department can mean a problem for another one.

The most commonly used technique for analyzing risk is the so-called "scenario analysis". This simply consists of the probability of the event and the impact this would have on the company. The scenario analysis is just one of many approaches to analyzing risks, for example in the matrix, the failure mode and effects analysis (FMEA) or the program evaluation and review technique (PERT).

To properly perform a risk evaluation it firstly should be defined which levels will be used for evaluating the risks. For example, there should be a range between 1 and 5 to signify the impact or the likelihood a certain "size". If one wants a more detailed evaluation the range could be extended to between 1 and 20. If one requires a more exact evaluation, there could be also a more exact classification of what a 'very low impact' means. This could be described by letters and for probability or affected costs percentages also could be stated for the different evaluation levels (see figure 6).

Project Objective	1 Very Low	2 Low	3 Moderate	4 High	5 Very High
Cost	Insignificant cost increase	< 10% cost increase	10-20% cost increase	20-40% cost increase	> 40% cost increase
Time	Insignificant time increase	< 5% time increase	5-10% time increase	10-20% time increase	> 20% time increase
Scope	Scope decrease barely noticeable	Minor areas of scope affected	Major areas of scope affected	Scope reduction unacceptable to sponsor	Project end item is effectively useless
Quality	Quality degradation barely noticeable	Only very demanding applications are affected	Quality reduction requires sponsor approval	Quality reduction unacceptable	Project end item is effectively useless

Figure 6: Evaluation of Risks

The evaluation form can be filled in by management or with the help of an expert. Techniques used are versatile and range from exact point estimations to workshops. Beside the most probable case, the worst case and the best case are also estimated.

To make risk analysis more demonstrative, the organization can use the matrix to show the importance of several risks. The matrix indicates two aspects of the considered risk: the impact it would have and the probability of its occurrence. An often used matrix has 5 times 5 fields, each with another value of probability and impact (see figure 7). As each combination has another meaning for the project, accordingly the matrix is divided into light grey, white and dark grey zones. White stands for moderate risks and green for minor risks. As one can see, the dark grey colored zone is arranged on the right and the white zone on the left, where the impact is lower. In between the white can be found the dark grey zone which is very low in the probability menu because the impact is still so high although the probability is low. In general one can say the impact is more important as this comparison shows a 10% probability of losing 1 Mio. € is considered to be a more serious risk than a 90% probability of losing 1000 €.

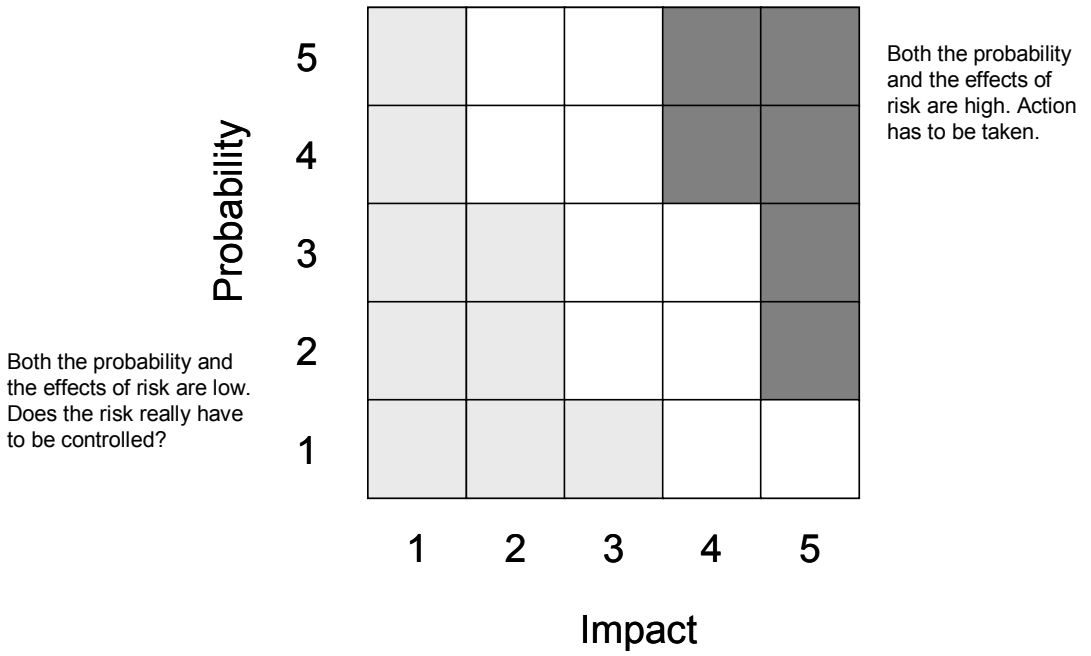

Figure 7: Risk Matrix

With the help of this matrix management can act to prioritize the risks so that they know which risks should be addressed particularly and at first. Prioritization also helps to adopt the given means reasonably, which is very important as all resources in management such as material, financials, human resources and time are highly limited.

The FMEA (Failure mode and effects analysis) model is similar to the matrix but extends the impact and probability by the detection possibility, meaning how hard it is to actually realize the occurring risk. The equation enlarged with detection is:

$$\text{Impact} \times \text{Probability} \times \text{Detection} = \text{Risk Value}$$

Enterprise Risk Management

To make the equation work, each of the dimensions has to be evaluated by a five-point scale. Detection describes the ability of the project team to detect that the risk is threatening. At the 1 to 5 scale "1" would mean easy to detect and "5" that the detection would probably only take place when it is too late to react. The product of the data would have a range between 1 and 125. '1' shows the risk has a low probability, with an impact of level 1 and would be easy to detect. At the other extreme the result '125' would show that the team had to handle a high-impact risk with high probability and which is nearly impossible to detect. This would mean management needs to think about whether or not to start the project if the risk could not be mitigated or transferred. All in all, the range between 1 and 125 can be used to define the hazardous nature of a risk.

PERT (Program evaluation and review technique) was developed within the framework of the U.S. Navy's Polaris-project. Nobody knew how long it would take to produce the parts for the rocket. There were many new parts coming from the R&D. To solve the problem of planning the team asked all suppliers to estimate the duration of production. It is assumed that with help of the program evaluation and review technique the Polaris rocket was accomplished after two years which is about 45% earlier than first estimated.

PERT is similar to the critical path method (CPM) known from the scheduling theory. The methods were developed at nearly the same time. The difference is that CPM uses the most frequent duration and is used for standardized projects. In contrast to that, PERT is used for projects with high uncertainty and little experience. PERT is utilized to compute the probability of meeting different project durations.

PERT is useful as it provides the expected project completion time and the probability of the completion before a specified date. Furthermore, it helps in ascertaining which activities have slack time and those which can lend resources to critical activities. Disadvantages are that the estimates can be somewhat subjective and also depend upon the experience of the project members. Furthermore, the beta distribution might not always match the reality. It is said that PERT often underestimates the project completion time because other paths than assumed previously can become critical paths if the related activities be behind schedule.

2.4.3 Risk Response

After having collected all data for the risk control, a risk might occur once. As a result, management has to decide how to react to it. The literature defines five main alternatives between which one can choose: **mitigate, avoid, transfer, share** or **retain** the risk are the main possibilities.

To **mitigate** the risk means to reduce the impact and risk of occurrence. This is something one can already do in normal operational business. If one detects a risk one knows could be reduced, there are two alternatives: the probability of the occurrence of the risk could be reduced or the impact of the risk, having occurred, could be minimized. Normally one would firstly endeavor to reduce the probability of the risk and, failing that, one would attempt to reduce the impact. The last mentioned is more expensive and perhaps it is not even necessary to consider whether probability could be reduced significantly.

Two terms familiar especially from engineering projects are ‘testing’ and ‘prototyping’. One can test the project in a smaller format with less risk and thereby detect possible failures and problems. With the help of the team one can prepare for these problems or even eliminate them before starting the real project work. Of course there will be some unanticipated problems when implementing the project as at that time the levels of complexity are higher.

Two things which cannot be mitigated too easily are cost and time as money is used up and days are numbered. But there is a solution: budget reserves and time buffers. Before this is done one always identifies a kind of safety ratio. This ratio is often directly related to the experience gained from recent projects.

Avoiding risk is a more drastic approach as the whole business plan might be changed to avoid a particular risk. One should consider carefully whether such a risk is so important that changes to the plan are warranted. An example of how to avoid a risk could be utilizing well known technology instead of new experimental technology even though the experimental technology might have made some processes easier.

With **risk transfer** the risk is just moved but not eliminated or dampened. One very common approach for risk transfer is outsourcing which is done nearly to excess in some industries. In that case the contractor has to take the risk. Besides the fact that of course the risk transfer will cost money – as the contractor also has to include the risk possibility in his pricing – it could be challenging to ensure the subcontractor is able to deal with the risk.

Another well known approach to **transfer risks** is contracting insurance. This may work well for some specific cases but for management in general it is not the right approach. Contracting insurance for a project or D&O insurances for executive liability can be used for low-probability and high-impact events. As these are somehow often acts of God they are more easily defined (e.g. an earthquake), but for day-to-day business risk insurances these are too expensive and the risks could not be described exactly enough.

Sharing risk, as the name implies, means that different parties share the risk of the same business plan, thereby allocating the risk between them. One well known example of this is Airbus. Airbus spread the risk through its various R&D departments over different countries like France, Britain and Germany.

Another kind of sharing the risk is signing a BOOT contract. BOOT is an acronym for "Build-Own-Operate-Transfer", e.g., a company is building a plant and after that the organization it is the owner until the operations are running smoothly and the whole check-up is done. Only if all these steps are successful is the ownership transferred to the client.

Sharing risks is also one way of saving money. This approach is often used in the field of logistics. Combining the ideas of subcontractors with your own could result in a major improvement, but in order to reach a level of teamwork where these procedures succeed, both sides should obtain advantages out of such a relationship. This is also one reason why partnerships can emerge. With both sides taking on the risk, the benefits coming from these new shared ideas are most probably equal.

The last option, **retaining** a risk, sounds a bit strange at first sight that, but there are cases where retaining and accepting the risk can be the easiest way to handle it. The possibility for such events is often so low that the risk could be accepted. In practice the impact of the risk is so low that it is easier to buffer it with for example financial reserves and to just keep on working.

With the help of buffers and reserves, some risks could be taken on should they appear. It could be easier to take the risk in this manner instead of trying unsuccessfully to transfer or reduce that risk. In a few cases the occurrence of the event could be ignored totally.

A contingency plan provides a safety net if one of the known risks becomes reality. With the help of that plan the action that should be followed is already made clear before the risk appears. This helps one to stay calm and find a step-by-step solution which can even reduce or weaken the impact of the event. The contingency plan should say what, when and where actions are to be taken. With the help of the contingency plan, the manager who has responsibility for dealing with such problems does not have to hastily invent a solution which in all likelihood would be a low quality solution. It is much easier if one can look into the contingency plan where the steps to be taken are described after having been well thought out during the project planning phase. The availability of a contingency plan can significantly increase the chances for project success.

At first sight it might seem easy: just plan the risks and it's done, but there are some conditions one must consider. First of all, proper documentation of the steps to be taken is absolutely necessary. Within that documentation cost estimations and the probable source should be named. Furthermore, the teams involved should agree upon the plan and the allocation of tasks should be made clear. All these steps should be followed to ensure all team members know what they are to do and are committed to the work, especially in the case of an emergency.

One simple way to follow all these instructions is to make a note of the information within a so-called risk response matrix. There is a more extreme possibility one has to take into account during risk contingency planning: There is the possibility that the risk remains after a risk response is made in accordance with the contingency plan.

2.4.4 Risk Control

The very last step in the whole risk management process is risk control. Included in this step are the execution of the risk response strategy, monitoring and triggering events, initiating contingency plans, and remaining alert to new risks. The management system is also essential in risk control. During the process there might be changes in scope, budget and schedule of the project with which management has to deal.

It is also the duty of management place equal importance on monitoring all possible risks and enhancing the business' development. Risk assessment and updating should be part of every status meeting and progress report system. Also, management and all employees should always be aware that unpredictable risks may occur. But this is not the usual case in daily business. Team members are not always willing to find out new risks and problems. If the organization's culture is one where one is punished by management for mistakes made, then it is clear that employees will be reluctant to speak about them for fear that these problems reflect badly on their performance. The tendency to suppress such important information is higher when responsibilities are unclear and employees are under great time pressure from top management to finish their work within a short time frame.

So it is the duty of management to create an environment in which all employees feel free to raise concerns and admit mistakes. This should be the standard aimed for in every business, because hiding risks and/or denying problems can inhibit the future success of the company. Everybody should be encouraged to identify problems and new risks and therefore the project manager must have a positive attitude toward risk.

In very complex and huge company environment, the risk identification and assessment step has to be repeated on a regular time basis. Outside stakeholders and experts should be brought into the discussion so that they can review the actual risk profiles.

Another useful key success factor is the assignment of responsibility for every identified risk. This step can be very complicated in the case of multiple organizations being involved. Without responsibility being assigned for each identified risk, nobody really feels responsible or takes responsibility for dealing with that occurred risk. The responsibility is then passed one to another, with each person saying "this is not my work." This mentality is very dangerous for overall business performance. Therefore it is very important that responsibility for each identified risk is assigned by mutual agreement between all relevant stakeholders so that everyone knows who is dealing with each risk. If the whole risk management process is not formalized, the response to and the responsibility for certain risks will simply be ignored.

Audits usually are an important part of risk response control. Audits can be defined as systematic and independent analyses. The term "audit" has its origin in the Latin language. The Latin word "audire" means "hear", so a quality audit is a "quality hearing". Through audits one can check whether quality-related work and the results gained through such work conform to the standards and to the planned requirements. An audit checks whether the work is done economical and rational. The main aim of audits is to discover weak points and risks inside an organization or project. A big advantage of audits is the ability to check quality-related issues and workflow in a very good way. A disadvantage is the amount of preparation and the time demand for preparation of the paperwork and training of employees. However audits only allow a short snap-shot of the situation. Some employees consider that it is a critique about the work they did and may develop a grudge against the auditor.

Every audit results in an audit report. Internal reports must contain for example the basic information and procedures of the evaluation and observations in terms of project documentation or personnel qualification. Non-conformities also must be reported. This is necessary to enable the next auditor to check whether corrective actions have been considered. Furthermore a list of participants must be included in an audit report.

Another major part of the risk control process is the establishment of a changed management system. It is common that the project will not materialize in the way originally planned or envisaged. There are many sources of changes that possibly could affect your project and its course. Usually you could categorize these changes into one of the following categories:

- Changes in Scope: For example the project customer wants to implement an additional feature or a change in design which represents a major challenge.
- Implementation of contingency plans: In this situation a risk actually occurred. Now actions to counteract this risk have to start. These actions need resources in terms of cost and schedule and so represent a change to the baseline.
- Improvement changes by project team members: For example a change in suppliers. A new supplier can deliver items more cheaply but of the same quality.

Enterprise Risk Management

All changes usually represent big challenges to the whole team and management. Often change to a project is unavoidable and therefore a well-defined change review and control process in the early stages of a project is required. These control processes include reporting, controlling and recording changes to the baseline of the project. Most change control systems are designed to fulfill the following points:

- Identify proposed changes
- List expected effects of proposed changes on schedule and budget
- Review, evaluate, and approve or disapprove changes formally
- Negotiate and resolve conflicts of change, conditions and cost
- Communicate changes to parties affected
- Assign responsibility for implementing change
- Adjust master schedule and budget
- Track all changes that are to be implemented

In general, stakeholders in the communication plan, which is defined in advance, will determine the communication and decision-making processes which must be used to in order to make any changes to the project. The decision-making process may vary between bigger and smaller companies. In larger companies it could be that, for instance, when you want to change important requirements of your departmental plan you need multiple sign-offs from different stakeholder whereas switching a single supplier could be done by the manager himself because he has the authorization to do so.

Never neglect the impact of changes. Very often several solutions have adverse effects. Therefore all changes must be assessed by people with the appropriate knowledge and qualifications in their respective fields.

Every accepted change must be integrated into the plan of record through changes in the WBS (work breakdown structure) and baseline schedule. The plan of record is the current reference in terms of schedule, costs and scope. If the change control system is not integrated with the WBS and baseline, sooner or later the business plan and control system will cease to work. The key success factor for the change control system is to document every single change as it occurs. Benefits of these requirements are:

- Inconsequential changes are discouraged by the formal process
- Costs of changes are maintained in a log
- Integrity of the WBS and performance measures is maintained
- Allocation and use of budget and management reserve funds are tracked
- Responsibility for implementation is clarified
- Effect of changes is visible to all parties involved
- Implementation of change is monitored
- Scope changes will be quickly reflected in baseline and performance measures

Change control is important within the business' / department's plan. As the business matures there must be a person who or group which is responsible for approving the changes, keeping documents updated, and communicating all changes to the relevant stakeholders. Success depends heavily upon keeping the change control process updated.

2.5 Risk Culture

The best system of risk management remains ineffective if it is not 'lived' every single day within the company. The lived risk culture is one of the most lasting instruments for a company. The risk culture – as a share of the company culture – determines how the employees behave in dealing with risks: Do they perceive the risks consciously? Do they make their decisions from the risk point of view? To extend the risk culture in their own company, executives have to demonstrate that they have exemplary functions and that they can lay the foundation for open communication with their management style. In this atmosphere colleagues dare to respond to risks. The company's suitable exchange and communication possibilities must provide an atmosphere of risk sharing culture between employees and management.

Many companies which suffered through the recent financial crisis have come to recognise the weaknesses within their risk management systems. However, most companies only dragged up to now none or only half-hearted consequences.

3 Conclusion and Outlook

Bad or no risk management often costs the company their very existence. Unfortunately, risk management is looked upon by many companies merely as a legal necessity rather than a value-adding strategy. Besides, as the use is not recognized, often ERM is only done to fulfill regulatory requirements for risk management, with minimum expenses. Such an approach neglects the fact that not-handled risks can become an enormous expense factor. However, the effort involved in establishing a well-defined and well-running enterprise risk management system is enormous. But it is a definitely worth paying.

Shareholder and stakeholder values are maximized if executives marry strategies and approaches which allow an optimum balance between turnover, growth and profit with the associated risks. A financially effective insertion of resources within the organisation can be achieved. Enterprise risk management includes:

- **Alignment of risk and strategy** – executives consider the risk incline of the organisation by the assessment of strategic alternatives and by the development of mechanisms towards the control of the risks.
- **Improvement from risk-based decisions** – enterprise risk management provides alternatives in case a risk is detected – risk avoidance, risk reduction, risk distribution and risk acceptance.
- **Reduction in surprises and losses in the business environment** – organizations improve their ability to recognize possible events and to initiate counteractive measures as well as to reduce surprises and the expenses or losses involved with them.
- **Determination and control of multiple and cross-company risks** – every company faces a huge number of risks in which several departments are concerned. Parallel to this, company-wide risk management allows effective reactions dependent on each other as well as on general measures with multiple risks.
- **Use of chances** – considering all possible events allows executives to recognize chances and to react proactively.
- **Improved capital allocation** – reliable risk information permits executives to assess the capital and to attract investors.

Enterprise risk management is an ongoing process and many managers have learned their lesson the hard way: risk never sleeps.

In the near future the pressure on companies will further rise to realize additional measures for risk management. The American stock market supervisory body, SEC, today requires from every company an annual report which state's the company's position with regard to specific risks within the industry and the company. One can assume that the European supervisory authorities will soon make similar regulations. The general risk consciousness of people and organizations is on the rise. Today one is ready to incur major expense in order to lower risks. Every company must allow for the fact that it will be called to account sometime in the future if it takes risks which cannot be known or quantified today.

However, we should not concentrate too strongly upon risks and thereby miss chances. The fact that risk management is especially in that danger has been stressed by the sociologist Perrow again and again: To Perrow, big risks originate always when a system crosses a certain complexity and the components of that system are strongly coupled with each other. Nobody can overlook a complicated system. Therefore, there can't be a central instance which can quickly initiate measures towards risk lowering in a crisis. Decisions must be decentralized where the detailed knowledge exists. If the single elements of the system are linked strongly with each other, a decentralized place does not know what effect a local decision on the whole system has.

How does management react? Ordinarily one tries to absorb risks with a back-up system. New nuclear power plants dispose of a several times protected reactor block. In a car the brakes might not be enough, so we complement these with seat belts and air bags. However, risk increases proportionately with every increase in the complexity of a system. We are faced with a dilemma. We have an analogous development in Enterprise Risk Management. Obviously, even with internal audit, external audit, accountancy and controls, disasters like Enron can occur, so we complement the existing systems with a back-up- risk management, and hope that the dilemma of Perrow does not eventuate.

We should not improve existing systems constantly bit-by-bit if new and easier systems are available to us. It is to be hoped that risk management serves in the future to screw back not only complexity, but to develop new, easier systems which are basically as safe as traditional structures.