RISK MANAGEMENT: PROCEDURES, METHODS AND EXPERIENCES

Heinz-Peter Berg
•
Bundesamt für Strahlenschutz, Salzgitter, Germany

e-mail: hberg@bfs.de

ABSTRACT

Risk management is an activity which integrates recognition of risk, risk assessment, developing strategies to manage it, and mitigation of risk using managerial resources. Some traditional risk managements are focused on risks stemming from physical or legal causes (e.g. natural disasters or fires, accidents, death). Financial risk management, on the other hand, focuses on risks that can be managed using traded financial instruments. Objective of risk management is to reduce different risks related to a pre-selected domain to an acceptable. It may refer to numerous types of threats caused by environment, technology, humans, organizations and politics. The paper describes the different steps in the risk management process which methods are used in the different steps, and provides some examples for risk and safety management.

1 INTRODUCTION

1.1 Risk

Risk is unavoidable and present in every human situation. It is present in daily lives, public and private sector organizations. Depending on the context (insurance, stakeholder, technical causes), there are many accepted definitions of risk in use.

The common concept in all definitions is uncertainty of outcomes. Where they differ is in how they characterize outcomes. Some describe risk as having only adverse consequences, while others are neutral.

One description of risk is the following: risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organization's objectives.

The phrase "the expression of the likelihood and impact of an event" implies that, as a minimum, some form of quantitative or qualitative analysis is required for making decisions concerning major risks or threats to the achievement of an organization's objectives. For each risk, two calculations are required: its likelihood or probability; and the extent of the impact or consequences.

Finally, it is recognized that for some organizations, risk management is applied to issues predetermined to result in adverse or unwanted consequences. For these organizations, the definition of risk which refers to risk as "a function of the probability (chance, likelihood) of an adverse or unwanted event, and the severity or magnitude of the consequences of that event" will be more relevant to their particular public decision-making contexts.

1.2 Risk Management

Two different safety management principles are possible: consequence based safety management will claim that the worst conceivable events at an installation should not have consequences outside certain boundaries, and will thus design safety systems to assure this. Risk based safety management (usually called risk management) maintains that the residual risk should be analysed both with respect to the probabilistic and the nature of hazard, and hence give information for further risk mitigation. This implies that very unlikely events might, but not necessarily will, be tolerated.

Risk management is not new tool and a lot of standards and guidance documents are available (ACT 2004, AZ/NZS 2004, Committee 2004, DGQ 2007, FAA 2007, HB 2004, IEC 2008, ON 2008, Rio Tinto 2007, Treasury Board of Canada 2001). It is an integral component of good management and decision-making at all levels of an organization. All departments in an organization manage risk continuously whether they realize it or not, sometimes more rigorously and systematically, sometimes less. More rigorous risk management occurs most visibly in those departments whose core mandate is to protect the environment and public health and safety. At present, a further generic standard on risk management is in preparation as a common ISO/IEC standard (IEC 2007) describing a systemic top down as well as a functional bottom up approach (see Fig. 1) This standard is intended to support existing industry or sector specific standards.

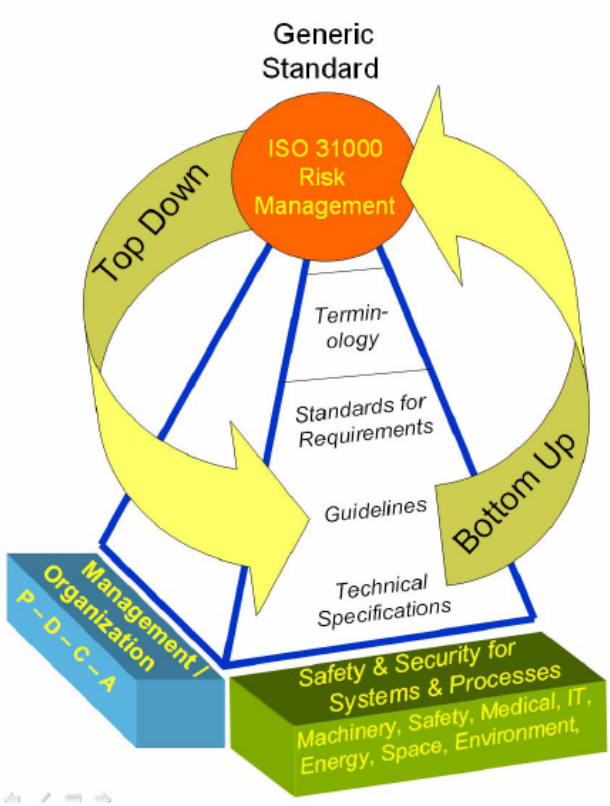

Figure 1. Approach of the planned generic standard on risk management.

As with the definition of risk, there are equally many accepted definitions of risk management in use. Some describe risk management as the decision-making process, excluding the identification and assessment of risk, whereas others describe risk management as the complete process, including risk identification, assessment and decisions around risk issues.

One well accepted description of risk management is the following: risk management is a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues.

In order to apply risk management effectively, it is vital that a risk management culture be developed. The risk management culture supports the overall vision, mission and objectives of an organization. Limits and boundaries are established and communicated concerning what are acceptable risk practices and outcomes.

Since risk management is directed at uncertainty related to future events and outcomes, it is implied that all planning exercises encompass some form of risk management. There is also a clear implication that risk management is everyone's business, since people at all levels can provide some insight into the nature, likelihood and impacts of risk.

Risk management is about making decisions that contribute to the achievement of an organization's objectives by applying it both at the individual activity level and in functional areas. It assists with decisions such as the reconciliation of science-based evidence and other factors; costs with benefits and expectations in investing limited public resources; and the governance and control structures needed to support due diligence, responsible risk-taking, innovation and accountability.

A typical decision support for risk and safety management at strategic, normative and operational level is provided in (JCSS 2008).

1.3 Integrated Risk Management

The current operating environment is demanding a more integrated risk management approach (see Bolvin et al. 2007 and Treasury Board of Canada 2001). It is no longer sufficient to manage risk at the individual activity level or in functional silos. Organizations around the world are benefiting from a more comprehensive approach to dealing with all their risks.

Today, organizations are faced with many different types of risk (e.g., policy, program, operational, project, financial, human resources, technological, health, safety, political). Risks that present themselves on a number of fronts as well as high level, high -impact risks demand a co-ordinated, systematic corporate response.

Thus, integrated risk management is defined as a continuous, proactive and systematic process to understand, manage and communicate risk from an organization-wide perspective. It is about making strategic decisions that contribute to the achievement of an organization's overall corporate objectives.

Integrated risk management requires an ongoing assessment of potential risks for an organization at every level and then aggregating the results at the corporate level to facilitate priority setting and improved decision-making. Integrated risk management should become embedded in the organization's corporate strategy and shape the organization's risk management culture. The identification, assessment and management of risk across an organization helps reveal the importance of the whole, the sum of the risks and the interdependence of the parts.

Integrated risk management does not focus only on the minimization or mitigation of risks, but also supports activities that foster innovation, so that the greatest returns can be achieved with acceptable results, costs and risks.

From a decision-making perspective, integrated risk management typically involves the establishment of hierarchical limit systems and risk management committees to help to determine the setting and allocation of limits. Integrated risk management strives for the optimal balance at the corporate level. However, companies still vary considerably in the practical extent to which important risk management decisions are centralised (Basel Committee on Banking Supervision 2003).

1.4 Safety management

Apart from reliable technologies, the operational management of a industrial plant with high risk potential is also a highly important factor to ensure safe operation. Owing to the liberalisation of the markets and resulting cost pressure to the industries, the importance of operational management is growing since cost savings in the areas of personnel and organization result in reducing the number of personnel together with changes in the organizational structure and tighter working processes.

For small- and medium-sized companies, specific support is necessary and provided in (Rheinland-Pfalz 2008).

Experience with accidents in different branches of industry shows the importance of safe operational management. Today, effective safety management is seen as one crucial element of safe operational management (Hess & Gaertner 2006).

The term safety management subsumes the entirety of all activities relating to the planning, organization, management and supervision of individuals and work activities with a view to the efficient achievement of a high degree of safety performance, i.e. the achievement of a high quality of all activities that are important to safety, and to the promotion of a highly developed safety culture. Safety management is not limited to certain organization units but comprises the entire safety-related organization of the company. Safety management is the responsibility of the management level of a company.

For example in case of nuclear power plant in Germany (see ICBMU 2004), the licensee is according to the Atomic Energy Act responsible for the safety of the plant he operates. To fulfil the conditions associated with this responsibility, he has to implement an effective safety management system that complies with the requirements of the current regulations and with international standards. Typical management systems in nuclear power plants are described in (GRS 2007).

Sometimes risk management and safety management are seen as the same type of management, but in practice safety management is a main and important part of the risk management which also covers, e.g. financial risks.

2 RISK MANAGEMENT STEPS AND TOOLS

The risk management steps (see Fig. 2) are:

1. Establishing goals and context (i.e. the risk environment),
2. Identifying risks,
3. Analysing the identified risks,
4. Assessing or evaluating the risks,
5. Treating or managing the risks,
6. Monitoring and reviewing the risks and the risk environment regularly, and
7. Continuously communicating, consulting with stakeholders and reporting.

Some of the risk management tools are described in (IEC 2008) and (Oehmen 2005).

2.1 Establish goals and context

The purpose of this stage of planning enables to understand the environment in which the respective organization operates, that means to thoroughly understand the external environment and the internal culture of the organization. The analysis is undertaken through:

- establishing the strategic, organizational and risk management context of the organization, and
- identifying the constraints and opportunities of the operating environment.

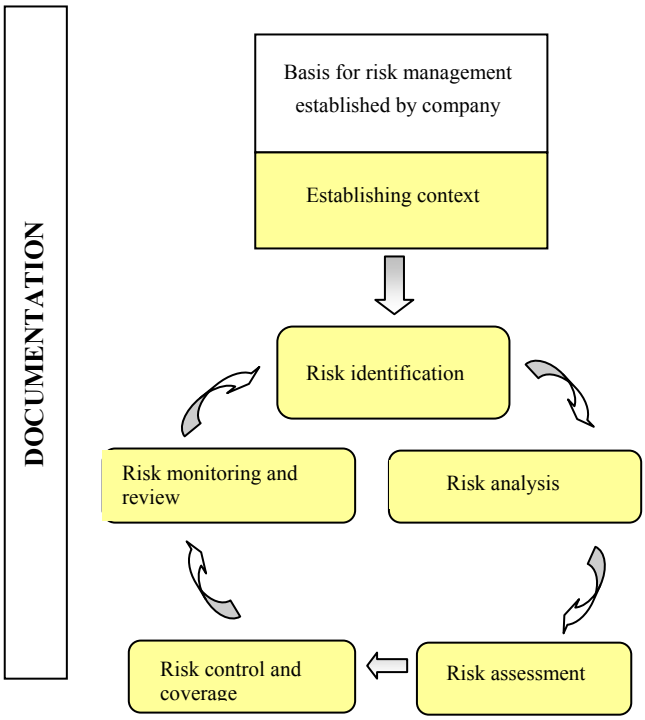

Figure 2. Risk management process.

The establishment of the context and culture is undertaken through a number of environmental analyses that include, e.g., a review of the regulatory requirements, codes and standards, industry guidelines as well as the relevant corporate documents and the previous year's risk management and business plans.

Part of this step is also to develop risk criteria. The criteria should reflect the context defined, often depending on an internal policies, goals and objectives of the organization and the interests of stakeholders. Criteria may be affected by the perceptions of stakeholders and by legal or regulatory requirements. It is important that appropriate criteria be determined at the outset.

Although the broad criteria for making decisions are initially developed as part of establishing the risk management context, they may be further developed and refined subsequently as particular risks are identified and risk analysis techniques are chosen. The risk criteria must correspond to the type of risks and the way in which risk levels are expressed.

Methods to assess the environmental analysis are SWOT (Strength, Weaknesses, Opportunities and Threats) and PEST (Political, Economic, Societal and Technological) frameworks, typically shown as tables.

2.2 Identify the risks

Using the information gained from the context, particularly as categorised by the SWOT and PEST frameworks, the next step is to identify the risks that are likely to affect the achievement of the goals of the organization, activity or initiative. It should be underlined that a risk can be an opportunity or strength that has not been realised.

Key questions that may assist your identification of risks include:

- For us to achieve our goals, when, where, why, and how are risks likely to occur?
- What are the risks associated with achieving each of our priorities?
- What are the risks of not achieving these priorities?
- Who might be involved (for example, suppliers, contractors, stakeholders)?

The appropriate risk identification method will depend on the application area (i.e. nature of activities and the hazard groups), the nature of the project, the project phase, resources available, regulatory requirements and client requirements as to objectives, desired outcome and the required level of detail.

The use of the following tools and techniques may further assist the identification of risks:

- Examples of possible risk sources,
- Checklist of possible business risks and fraud risks,
- Typical risks in stages of the procurement process,
- Scenario planning as a risk assessment tool ,
- Process mapping, and
- Documentation, relevant audit reports, program evaluations and / or research reports.

Specific lists, e.g. from standards, and organizational experience support the identification of internal risks. To collect experience available in the organization regarding internal risks, people with appropriate knowledge from the different parts of the organization should be involved in identifying risks. Creativity tools support this group process (see Fig. 3).

The identification of the sources of the risk is the most critical stage in the risk assessment process. The sources are needed to be managed for pro-active risk management. The better the understanding of the sources, the better the outcomes of the risk assessment process and the more meaningful and effective will be the management of risks.

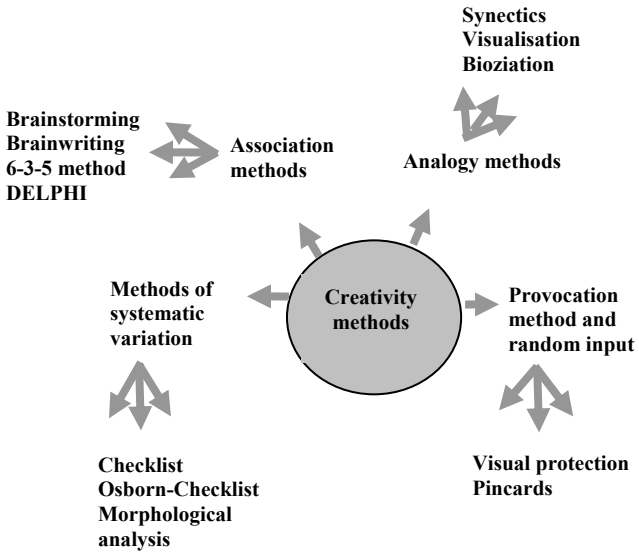

Figure 3. Creativity tools.

Key questions to ask at this stage of the risk assessment process to identify the impact of the risk are:

- Why is this event a risk?
- What happens if the risk eventuates?
- How can it impact on achieving the objectives/outcomes?

Risk identification of a particular system, facility or activity may yield a very large number of potential accidental events and it may not always be feasible to subject each one to detailed quantitative analysis. In practice, risk identification is a screening process where events with low or trivial risk are dropped from further consideration.

However, the justification for the events not studied in detail should be given. Quantification is then concentrated on the events which will give rise to higher levels of risk. Fundamental

methods such as Hazard and Operability (HAZOP) studies, fault trees, event tree logic diagrams and Failure Mode and Effect Analysis (FMEA) are tools which can be used to identify the risks and assess the criticality of possible outcomes.

An example of a systematic method for identifying technical risks of a plant is the elaboration of a risk register where different types of risks and damage classes are correlated to local areas of a plant (cf. Fig. 4).

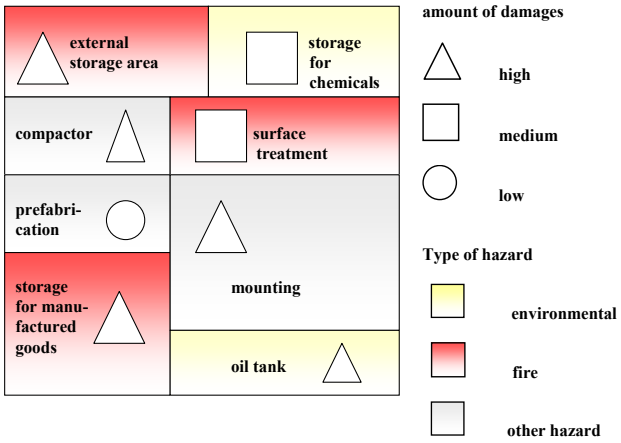

Figure 4. Example of a risk register.

2.3 Analyse the risk

Risk analysis involves the consideration of the source of risk, the consequence and likelihood to estimate the inherent or unprotected risk without controls in place. It also involves identification of the controls, an estimation of their effectiveness and the resultant level of risk with controls in place (the protected, residual or controlled risk). Qualitative, semi-quantitative and quantitative techniques are all acceptable analysis techniques depending on the risk, the purpose of the analysis and the information and data available.

Often qualitative or semi-quantitative techniques can be used for screening risks whereas higher risks are being subjected to more expensive quantitative techniques as required. Risks can be estimated qualitatively and semi-quantitatively using tools such as hazard matrices, risk graphs, risk matrices or monographs but noting that the risk matrix is the most common.

Applying the risk matrix, it is required to define for each risk its profile using likelihood and consequences criteria. Typical definitions of the likelihood and consequence are contained in the risk matrix (cf. Table 1).

Using the consequence criteria provided in the risk matrix, one has to determine the consequences of the event occurring (with current controls in place).

To determine the likelihood of the risk occurring, one can apply the likelihood criteria (again contained in the risk matrix). As before, the assessment is undertaken with reference to the effectiveness of the current control activities.

To determine the level of each risk, one can again refer to the risk matrix. The risk level is identified by intersecting the likelihood and consequence levels on the risk matrix.

Complex risks may involve a more sophisticated methodology. For example, a different approach may be required for assessing the risks associated with a significantly large procurement.

Table 1. Example of a risk matrix

Significance			Consequence				
			1 Insignificant Impact	2 Minor Impact to Small Population	3 Moderate- Minor Impact to Large Population	4 Major Impact to Small Population	5 Catastrophic – Major Impact to Large Population
Likelihood	1	Rare	Low	Low	Moderate	High	High
	2	Unlikely	Low	Low	Moderate	High	Very High
	3	Moderate / Possible	Low	Moderate	High	Very High	Very High
	4	Likely	Moderate	High	High	Very High	Extreme
	5	Almost Certain	Moderate	High	Very High	Extreme	Extreme

Special approaches exist to analyse major risk in complex projects, e. .g. described in (Cagno et al. 2007).

2.4 Evaluate the risk

Once the risks have been analysed they can be compared against the previously documented and approved tolerable risk criteria. When using risk matrices this tolerable risk is generally documented with the risk matrix. Should the protected risk be greater than the tolerable risk then the specific risk needs additional control measures or improvements in the effectiveness of the existing controls.

The decision of whether a risk is acceptable or not acceptable is taken by the relevant manager. A risk may be considered acceptable if for example:

- The risk is sufficiently low that treatment is not considered cost effective, or
- A treatment is not available, e.g. a project terminated by a change of government, or
- A sufficient opportunity exists that outweighs the perceived level of threat.

If the manager determines the level of risk to be acceptable, the risk may be accepted with no further treatment beyond the current controls. Acceptable risks should be monitored and periodically reviewed to ensure they remain acceptable. The level of acceptability can be organizational criteria or safety goals set by the authorities.

2.5 Treat the risk

An unacceptable risk requires treatment. The objective of this stage of the risk assessment process is to develop cost effective options for treating the risks. Treatment options (cf. Fig. 5), which are not necessarily mutually exclusive or appropriate in all circumstances, are driven by outcomes that include:

- Avoiding the risk,
- Reducing (mitigating) the risk,
- Transferring (sharing) the risk, and
- Retaining (accepting) the risk.

Avoiding the risk - not undertaking the activity that is likely to trigger the risk.

Reducing the risk - controlling the likelihood of the risk occurring, or controlling the impact of the consequences if the risk occurs.

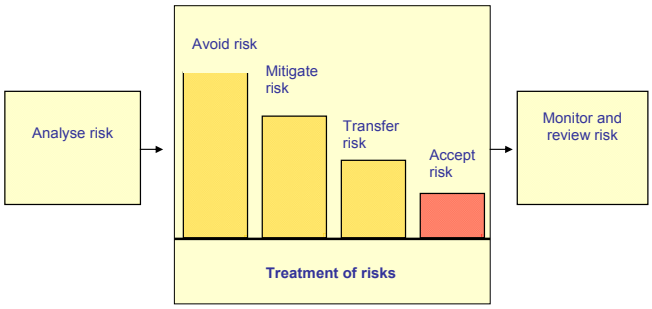

Figure 5. Treatment of risks

Factors to consider for this risk treatment strategy include:

– Can the likelihood of the risk occurring be reduced? (through preventative maintenance, or quality assurance and management, change in business systems and processes), or

– Can the consequences of the event be reduced? (through contingency planning, minimizing exposure to sources of risk or separation/relocation of an activity and resources).

Examples for the mitigation activity effectiveness are described in (Wirthin 2006).

Transferring the risk totally or in part - This strategy may be achievable through moving the responsibility to another party or sharing the risk through a contract, insurance, or partnership/joint venture. However, one should be aware that a new risk arises in that the party to whom the risk is transferred may not adequately manage the risk!

Retaining the risk and managing it - Resource requirements feature heavily in this strategy.

The next step is to determine the target level of risk resulting from the successful implementation of the preferred treatments and current control activities.

The intention of a risk treatment is to reduce the expected level of an unacceptable risk. Using the risk matrix one can determine the consequence and likelihood of the risk and identify the expected target risk level.

2.6 Monitoring the risk

It is important to understand that the concept of risk is dynamic and needs periodic and formal review.

The currency of identified risks needs to be regularly monitored. New risks and their impact on the organization may to be taken into account.

This step requires the description of how the outcomes of the treatment will be measured. Milestones or benchmarks for success and warning signs for failure need to be identified.

The review period is determined by the operating environment (including legislation), but as a general rule a comprehensive review every five years is an accepted industry norm. This is on the basis that all plant changes are subject to an appropriate change process including risk assessment.

The review needs to validate that the risk management process and the documentation is still valid. The review also needs to consider the current regulatory environment and industry practices which may have changed significantly in the intervening period.

The organisation, competencies and effectiveness of the safety management system should also be covered. The plant management systems should have captured these changes and the review should be seen as a ‘back stop’.

The assumptions made in the previous risk assessment (hazards, likelihood and consequence), the effectiveness of controls and the associated management system as well as people need to be monitored on an on-going basis to ensure risk are in fact controlled to the underlying criteria.

For an efficient risk control the analysis of risk interactions is necessary.

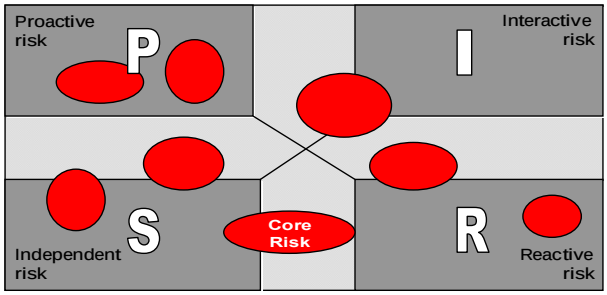

Figure 6. Results of a cross impact analysis.

This ensures that the influences of one risk to another is identified and assessed. Usual method for that purpose are a cross impact analysis (cf. Fig. 6), Petri nets or simulation tools.

A framework needs to be in place that enables responsible officers to report on the following aspects of risk and its impact on organizations´ operations:

– What are the key risks?
– How are they being managed?
– Are the treatment strategies effective? – If not, what else must be undertaken?
– Are there any new risks and what are the implications for the organization?

2.7 Communication and reporting

Clear communication is essential for the risk management process, i.e. clear communication of the objectives, the risk management process and its elements, as well as the findings and required actions as a result of the output.

Risk management is an integral element of organization´s management. However, for its successful adoption it is important that in its initial stages, the reporting on risk management is visible through the framework. The requirements on the reporting have to be fixed in a qualified and documented procedure, e. g., in a management handbook. The content of such a handbook is shown in Figure 7.

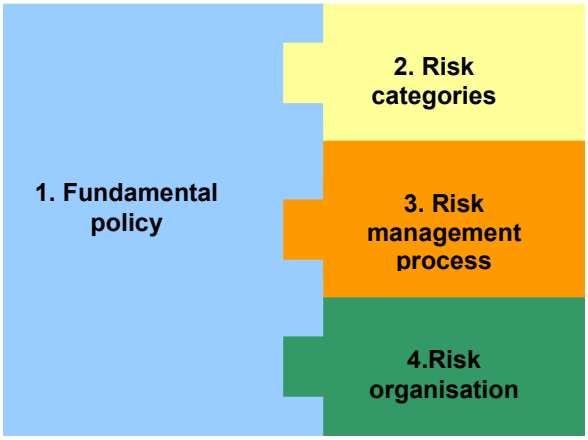

Figure 7. Structure of a risk management handbook.

Documentation is essential to demonstrate that the process has been systematic, the methods and scope identified, the process conducted correctly and that it is fully auditable. Documentation

provides a rational basis for management consideration, approval and implementation including an appropriate management system.

A documented output from the above sections (risk identification, analysis, evaluation and controls) is a risk register for the site, plant, equipment or activity under consideration. This document is essential for the on-going safe management of the plant and as a basis for communication throughout the client organisation and for the on-going monitor and review processes. It can also be used with other supporting documents to demonstrate regulatory compliance.

3 EXAMPLES

3.1 NASA risk management to the SOFIA programm

NASA and DLR (German Aerospace Center) have been working together to create the Stratospheric Observatory For Infrared Astronomy (SOFIA). SOFIA is a Boing 747SP (Special Performance) aircraft, extensively modified to accommodate a 2.5 meter reflecting telescope and airborne mission control system. In (Datta 2007) it is shown how the SOFIA program handled one safety issue through appropriate use of NASA`s Risk Management Process based on (NASA 2002).

3.1.1 Risk identification

The safety issue was identified while reviewing the Probabilistic Risk Assessment of a depressurization scenario in the telescope cavity. The failure scenario itself was previously known where a leak in the telescope cavity door seal sucks air out from the telescope cavity creating a negative pressure differential between the telescope cavity and the aft cavity. Two negative pressure relief valves were designed to handle this and other cavity negative pressure scenarios. However, the proposed new scenario had a leak area that was beyond the original design basis. Nevertheless, this failure scenario was deemed credible but with a lower probability of occurrence.

3.1.2 Risk analysis

After identification of the safety issue, both the risk management and the engineering processes required an analysis of this depressurization scenario. Multiple models of the depressurization scenarios were created and analyzed at peak dynamic pressures. The results revealed that under some failure scenarios the relief valves might not be redundant. Both valves need to function for adequate pressure equalization without exceeding structural design loads. These conditions created a program risk state that needed to be mitigated.

All considerations within the risk analysis were based on prescribed project risk definitions.

3.1.3 Risk control

As a result, the program started a risk mitigation plan where a test will be performed to characterize the seal failure scenario by intentionally deflating the seal at lower dynamic pressure.

This risk continues to reside in the SOFIA program risk list so as to ensure that the risk mitigation plan is carried out in the future. The risk list is the listing of all identified risks in priority order from highest to lowest risk, together with the information that is needed to manage each risk and document its evolution over the course of the program. The highest risks are extracted from the list. The negative pressure relief valve risk has not yet reached among the top fifteen list of risks (see Datta 2007).

3.2 Construction of a nuclear power plant

Risk identification and risk analysis can not only be performed on component or system level, but also for a comprehensive technical project such as a (nuclear) power plant.

3.2.1 Risk context

Since many years, no new nuclear power plant has been constructed in USA. However, in near future, decisions have to be made which types of power plants will reset the nuclear power plants which have to be shut down in the next ten years. Thus, for a new project the resulting risks have to be evaluated.

The risk context is determined by the electricity market, the license, the technical aspects of the design, the construction of the plant, the operation of the new plant as well as the financing of the project.

3.2.2 Risk identification

On the background of this context, a potential operator has to take into account the following risks:

– Licensing risks: will the plant be licensed in a predictable time schedule or will this be a longer procedure, which strongly influences the start of the commercial operation.

– Design risks: is the plant completely designed before construction or are surprises to be expected which lead to cost- intensive changes of the plant and delay of the construction period.

– Technical risks: will the plant behave as planned or will unknown technical problems lead to shut down and thus fail the projected goals.

– Cost risks: will the plant to more expensive as planned and the chances in the free electricity market reduced.

– Time schedule risks: will the plant start the production at the scheduled time or have delays to be expected.

– Finance risks: which possible uncertainties have to be taken into account by investors with respect to the new project, e.g., how is the public acceptance of a new nuclear power plant.

3.2.3 Risk analysis

In a specific case, General Electric has analysed the risk of constructing a new plant in the following manner:

– License risks: the new reactor type has been developed in accordance with current nuclear safety standards and is already certified site-independently by the US licensing authority. Moreover, this type of reactor has already been licensed in Japan, where two plants are running successfully since five years.

– Design risks: the reactor type is completely planned with all necessary drawings. Material and costs are exactly known.

– Technical risks: the plants constructed in Japan have a total operating time of ten years with a high availability.

– Finance risks: main problem is the financing of a new nuclear power plant project because of experiences in the eighties with construction times up to 15 years.

3.2.4 Risk evaluation

Following this risk analysis, an evaluation of the risks has been the next step:

– License risk: the experiences listed in the risk analysis lead to the expectations that the licensing process should not last more than one year.

– Design risk: due to the completely available design documentation no larger deviations are expected that result in expensive delays.

– Technical risk: the risk evaluation of the potential operator and the investors will not only be based on the expected high availability, but also on the occurrence frequency of an accident and the acceptance by the public in comparison with other energy producing systems.

3.2.5 Risk treatment

General Electric has chosen from the different alternatives to treat risks as described in 2.5 to retain and accept the risks for costs and time schedule by offering a fixed price and a construction time which will be determined in the contract.

3.3 National foresight program "Poland 2020"

Totally different and more global types of risk management are so-called foresight programs. Foresight means a systematic method of building a medium and long-term vision of development of the scientific and technical policy, its directions and priorities, used as a tool for making on-going decisions and mobilizing joint efforts. The aim of foresight is to indicate future needs, opportunities and threats associated with the social and economic growth and to plan appropriate measures in the field of science and technology.

The scope of realization of the National Foresight Programme “Poland 2020” (see Fig. 8) covers the three research areas “sustainable development of Poland”, “information and telecommunications technologies” and “security”.

Figure 8. Cover of the brochure describing the Polish foresight program.

The aim of the National Foresight Programme "Poland 2020" is to:

– lay out the development vision of Poland until the year 2020,

– set out – through a consensus with the main beneficiaries – the priority paths of scientific research and development which will, in the long run, have an impact on the acceleration of the social and economic growth,

– put the research results into practice and create preferences for them when it comes to allotting funds from the budget,

– adjust the Polish scientific policy to the requirements of the European Union,

– shape the scientific and innovative police towards knowledge-based economy.

For the purpose of foresight, different methods can be applied to prepare long-term development scenarios (see Table 2).

Foresight can never be completely dominated by quantitative methods: the appropriate mix of methods depends on access to relevant expertise and the nature of the issues.

Various foresight methods are planned to be used in the National Foresight Programme "Poland 2020", among which the following methods will be the leading ones:

– Expert panels,
– SWOT analysis,
– Delphi analysis,
– PEST analysis,
– Cross-impact analysis,
– Scenarios of development.

Table 2. Methods typically used for foresight programs

Categories by Criteria	Methods
Quantitative methods (use of statistics and other data) to elaborate future trends and impacts	– Trend extrapolation – Simulation modelling – Cross impact analysis – System dynamics
Qualitative methods (drawing on expert knowledge) to develop long term strategies	– Delphi method – Experts panels – Brainstorming – Mindmapping – Scenario analysis workshops – SWOT analysis
Methods to identify key points of action to determine planning strategies	– Critical/ key technologies – Relevance trees – Morphological analysis

3.4 Risk management in the sector of banks and insurance companies

Basel II and the Capital Requirements Directive (Committee for 2005) are especially important for banks and small and medium sized companies. Rules on capital requirements are designed to protect savers and investors from the risk of the failure or bankruptcy of banks. They ensure that these institutions hold a minimum amount of capital. The Capital Requirements Directive was adopted on 14 June 2006 and comes into force January 2007 with full implementation by 2008. Capital adequacy rules set down the amount of capital a bank or credit institution must hold. This amount is based on risk.

Therefore, it is expected that this rules will have an important influence on the establishment of a risk management system.

Three main issues of the Capital Requirements Directive are:

– the new directive is more risk sensitive,

– costs to smaller banks and consequently to small-company growth, where the EU lags other regions, and

– moral hazard concerns in that risks are partly passed to insurers and banks, unlike insurers have potential last resort support from central banks.

Some commentators argue that strengthening the capital base of banks and encouraging the management of risk does not reduce the risk but merely passes it on elsewhere. Credit risk in particular is being passed on to insurance companies and funds, which are in turn passing it on to householders, i. e., one can ask the question whether ultimately, it may be the consumer who stands to lose if things go wrong.

Comparable to Basel II for the banks and investment institutions will Solvency II fundamentally change and support risk management of the insurance companies. The requirements on the capital equipment will then depend on the risk profile of the insurance company. Besides the quantitative determination of the capital equipment it is part of Solvency II to determine the internal risk management.

Basis in economics and finance is the so-called value at risk (VaR) method. VaR is the maximum loss, not exceeded with a given probability defined as the confidence level, over a given period of time. Although VaR is a very general concept that has broad applications, it is most commonly used by security firms or investment banks to measure the market risk of their asset portfolios (market value at risk). VaR is widely applied in finance for quantitative risk management for many types of risk. VaR does not give any information about the severity of loss by which it is exceeded.

A variety of models exist for estimating VaR. Each model has its own set of assumptions, but the most common assumption is that historical market data is the best estimator for future changes. Common models include:

– variance-covariance, assuming that risk factor returns are always (jointly) normally distributed and that the change in portfolio value is linearly dependent on all risk factor returns,

– the historical simulation, assuming that asset returns in the future will have the same distribution as they had in the past (historical market data),

– Monte Carlo simulation, where future asset returns are more or less randomly simulated.

In (Taleb 2007 a, b), VaR is seen as a dangerously misleading tool. Two issues are mentioned with regard to conventional calculation and usage of VaR:

– Measuring probabilities of rare events requires study of vast amounts of data. For example, the probability of an event that occurs once a year can be studied by taking 4-5 years of data. But high risk-low probability events like natural calamities, epidemics and economic disasters (like the bank crash of 1929) are once a century events which require at least 2-3 centuries of data for validating hypotheses. Since such data does not exist in the first place, it is argued, calculating risk with any accuracy is not possible.

– In the derivation of VaR normal distributions are assumed wherever the frequency of events is uncertain.

Although many problems are similar for the banking and insurance sector respectively, there are some distinctions between these two kinds of companies. Banks mainly deal with bounded risks, e. g., facing credit risks. On the other hand, insurance companies often have to consider unbounded risks, e. g., when heavy-tailed distributed financial positions are present. To address both situations, one always treats integrable but not necessarily bounded risks in this work. Furthermore, a main issue will be to develop risk management tools for dynamic models. These naturally occur when considering portfolio optimisation problems or in the context of developing reasonable risk measures for final payments or even stochastic processes. One considers only models in discrete time and denotes these approaches with dynamic risk management. In dynamic

economic models one often faces a Markov structure of the underlying stochastic processes (Mundt 2008).

Systemic financial risk is the most immediate and the most severe. With so many potential consequences of the 2007 liquidity crunch unresolved, the outlook for the future is uncertain (WEF 2008).

The crisis of Société Générale in connection with the real estate credits in the US in 2007/2008 and the breakdown of further US banks in September 2008 might be a symptom for the fact that banks are underestimating the risks or do not apply the risk management tools in an appropriate manner.

4 CONCLUDING REMARKS

Risk management is, at present, implemented in many large as well as small and medium sized industries. In (Gustavsson 2006) it is outlined how a large company can handle its risks in practice and contains a computer based method for risk analysis that can generate basic data for decision-making in the present context. In that study, Trelleborg AB has been chosen as an example to illustrate the difficulties that can be encountered concerning risk management in a large company with different business areas. One typical difficulty is reaching the personnel. Another typical weakness is a missing system for controlling and following up on the results of the risk analysis that has been performed.

However, not only industries but also governmental organizations, research institutes and hospitals are now introducing risk management to some extent.

In case of hospitals. patient safety is endangered, e. g., by adverse events during medical treatment. Patient safety can be increased through risk management which reduces errors through error prevention. This presupposes the recognition of causes for errors and near misses which can be achieved through a critical incident reporting system (CIRS) with a detailed incident reporting form. CIRS is seen as an important instrument in the process of risk management and is, at present, of increasing importance and Switzerland and Germany.

Why is it important to have risk management in mind when performing risk assessment? The different tools support the answer to the following questions:

– risk analysis – how safe is the system, process or item to be investigated,

– risk evaluation – how safe is safe enough, e.g. by comparing the results of the risk analysis with prescribed safety criteria,

– risk management – how to achieve and ensure an adequate level of safety.

Thus, the results of technical risk assessments are one (often very important) part of an overall risk or safety assessment of an organization.

A further step is to couple knowledge management with risk management systems to capture and preserve lessons learned as described in (NASA 2007).

REFERENCES

[40] ACT Insurance Authority 2004. *Risk Management Toolkit.* February 2004.

[41] AZ/NZS 4360 2004. Risk Management. Standards Australia International Ltd, Sydney.

[42] Basel Committee on Banking Supervision 2003. Trends in Risk Integration and Aggregation, Basel, August 2003.

[43] Bolvin C., Farret, R., Salvi, O. 2007. Convergence towards integrated risk management: results from the European SHAPE-RISK project and other initiatives. Proc. ESREL 2007: 1683 – 1687.

[44] Cagno, E., Caron, F., Mancini, M. 2007. A multi-dimensional analysis of major risks in complex projects. Risk Management: 1–18.

[45] Committee for European Banking Supervisors 2005. Consultation Paper on the Supervisory Review Process under Pillar II of the Revised Basel Accord, Basel II), June 2005.

[46] Committee of Sponsoring Organizations of the Treadway Commission (ed.) 2004. Enterprise Risk Management – Integrated Framework – Application Techniques. September 2004.

[47] Datta, K. 2007. The application of the NASA risk management to the SOFIA program. Proc. Reliability and Maintainability Symposium 2007, Orlando, January 2007, 410 – 413.

[48] Deutsche Gesellschaft für Qualität e.V. 2007. Risk Management. DGQ 12 – 41, Beuth-Verlag, Berlin, April 2007 (in German).

[49] Federal Aviation Administration 2007. Safety Risk Management Guidance for System Organization. SRMGSA-Final Version 1.4a, February 2007.

[50] Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (ICBNU) 2004. Fundamentals of Safety Management Systems in Nuclear Power Plants. June 2004.

[51] Federation of European Risk Management Associations 2003. A Risk Management Standard.

[52] Gesellschaft für Anlagen- und Reaktorsicherheit mbH (GRS) 2007. Management Systems in Nuclear Power Plants. GRS-229, Cologne, August 2007 (in German).

[53] Gustavsson, H. 2006. A Risk Management Framework Designed for Trelleborg AB. Report 5195.

[54] HB 436 2004. Handbook Risk Management Guidelines. Standards Australia International Ltd., Sydney 2004.

[55] Hess, S.M., Gaertner, J. P. 2006. Application of risk management as a cornerstone in ensuring nuclear plant safety. Proc. of the 8th International Conference on Probabilistic Safety Assessment and Management, May, 14 – 18, 2006, New Orleans, paper PSAM-0477.

[56] International Electrotechnical Commission (IEC) 2008. Draft IEC 31010 Ed. 1.0, Risk Management – Risk Assessment Techniques. May 2008.

[57] International Standardization Organization 2007. Draft ISO 31000, Risk Management Guidelines on Principles and Implementation of Risk Management. Final version to be issued in 2009.

[58] Joint Committee of Structural Safety (JCSS) 2008. Risk Assessment in Engineering, Principles, System Representation and Risk Criteria. JCSS, June 2008.

[59] Mundt, A.P. 2008. Dynamic risk management with Markov decision process. Universitätsverlag Karlsruhe, 2008.

[60] NASA 2002. Risk Management Procedural Requirements. NPR 8000.4, April 2002.

[61] NASA 2007. Exploration Systems, Risk Management Plan. August 2007.

[62] Oehmen, J. 2005. Approaches to Crisis Prevention in Lean Product Development by High Performance Teams and through Risk Management. Munich, September 2005.

[63] Oesterreichisches Normungsinstitut 2008. ONR 49000 Risikomanagement für Organisationen und Systeme. (in German).

[64] Rheinland-Pfalz 2008. SGU-Leitfaden. (in German).

[65] Rio Tinto 2007. Risk Policy and Standard. August 2007.

[66] Taleb, N. 2007 a. The Black Swan: The Impact of the Highly Improbable. Penguin, London.

[67] Taleb, N. 2007 b. Epistemology and risk management. Risk & Regulation Magazine, Summer 2007.

[68] Treasury Board of Canada 2001. Integrated Risk Management Framework. April 2001.

[69] Wirthin, R. 2006. Managing Risk and Uncertainty: Traditional Methods and the Lean Enterprise. MIT/LAI, Presentation April 18, 2006.

World Economic Forum (WEF) 2008. Global Risks 2008, A Global Risk Network Report. Cologny/Geneva, January 2008.