Industrie Service

Choose certainty.
Add value.

Certification Standard CENARIOS®

Part A
General Requirements, Scope, Procedure, Documentation

Part B
Staff-Related Requirements

Part C
Organizational Requirements

Part D
Risk Assessment and Monitoring Requirements

Part E
Requirements Related to Risk Treatment and Risk Communication

Date: 2008-08-13

Our reference:
IS-ATC1-MUC/wei

Download

http://www.tuev-sued.de/uploads/images/1219824286015340810363/CENARIOS_Zertifiziergrundlage_e.pdf

Contact

nanotechnologie@tuev-sued.de

TÜV SÜD Industrie Service GmbH
Niederlassung München
Bereich Anlagentechnik
Risikomanagement
Westendstrasse 199
80686 Munich
Germany

Telefon: +49 89 5791 - 1235
Telefax: +49 89 5791 - 2888
www.tuev-sued.de
TÜV®

Supervisory Board:
Dr.-Ing. Axel Stepken (Chairman)
Board of Management:
Dr. Peter Langer (Spokesman)
Dipl.-Ing. (FH) Ferdinand Neuwieser

Headquarters: Munich
Trade Register: Munich HRB 96 869

Industrie Service

Choose certainty.
Add value.

CENARIOS® Certification Standard
Part A

Master Document

General Requirements
Scope, Procedure, Documentation

Date: 13 August 2008

Our references:
IS-ATC1-MUC

Document:
08-08-13 CENARIOS Certification Standard Part A.doc

This document consists of
17 pages
Page 1 of 17

.

Headquarters: Munich
Trade Register: Munich HRB 96 869

Supervisory Board:
Dr.-Ing. Axel Stepken (Chairman)
Board of Management:
Dr. Peter Langer (Spokesman)
Dipl.-Ing. (FH) Ferdinand Neuwieser

Telefon: +49 89 5791-0
Telefax: +49 89 5791-2888
www.tuev-sued.de

TÜV®

TÜV SÜD Industrie Service GmbH
Niederlassung München
Bereich Anlagentechnik
Westendstraße 199
80686 München
Deutschland

Table of Contents

0 Preamble

This master document of the CENARIOS® standard[1] for risk management certification is the generally applicable document for the assessment and certification of all risk management processes based on the CENARIOS® standard. It describes the requirements, in particular staff and organizational requirements that companies must satisfy when they implement a risk management system. Further key elements of the CENARIOS® standard are the criteria related to the assessment and treatment of risks.

This master document also provides an overview of the contents of the other documents of the CENARIOS® certification standard, parts B to E, and references other applicable documentation.

The CENARIOS® standard consists of the following parts

A General Requirements, Scope, Procedure, Documentation

B Staff-Related Requirements

C Organizational Requirements

D Risk Assessment and Monitoring Requirements

E. Requirements Related to Risk Treatment and Risk Communication

This document is part A of the CENARIOS® certification standard and provides those companies seeking to be certified with preliminary information in order to prepare for the certification process. Parts B to E of this standard contain more detailed information about the subjects addressed and aim to help companies identify opportunities for improvement, if necessary.

The CENARIOS® risk management system was especially developed for risk assessment in the nanotechnology sector. It covers the risks associated with the design and development, production and use of nanotechnology products and focuses on the following risk categories:

- Risks for staff producing and handling nanotechnology products (occupational health and safety), both at the producers of basic nanomaterials and at the companies which use and further process these nanomaterials.
- Production-related risks for the surroundings of the company and the environment;

  The two above risk categories are also referred to together as HSE risks[2].
- Consumer risks resulting from the use of nanotechnology products which may affect both company staff, users and third parties.

Certification according to this standard is restricted to the above risks and does not cover any other risks which must also be considered by companies, such as investment risks, liability risks and risks resulting from changes in legal or social framework conditions and/or corporate mismanagement.

In brief, the CENARIOS® risk management system aims to minimize the risks involved in nanomaterials or products in which nanomaterials are used for specific purposes. This certification standard defines the general requirements applicable to such a product-specific risk management system.

---

[1] CENARIOS® is the legally protected name of the risk management system developed jointly by TÜV SÜD and Innovationsgesellschaft, St. Gallen, Switzerland.

[2] HSE stands for Health, Safety and the Environment

1 Document Structure

The figure below summarizes the applicable documents of the CENARIOS® standards.

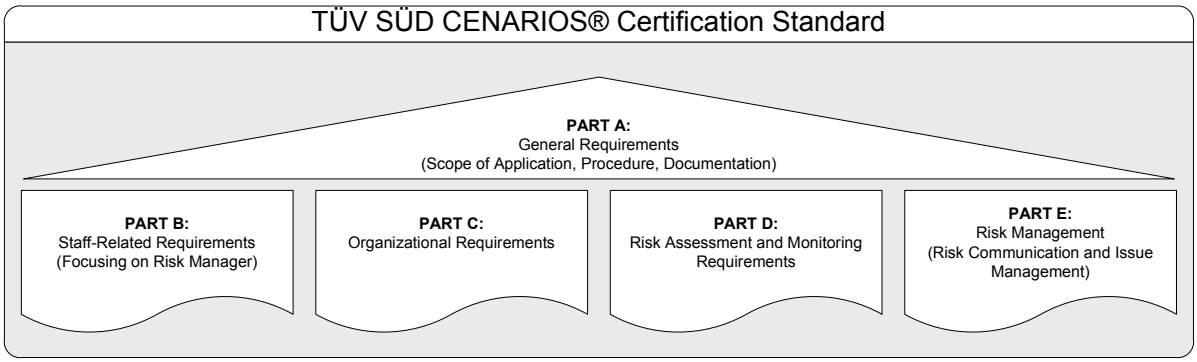

Figure 1-1 Document structure of the certification standard

1.1 Other applicable documents

Part A
Part A describes the general criteria and provides a summary of all subsequent parts of the standard. This part of the certification standard is based to some extent on *A Risk Management Standard* (FERMA).

Part B
Part B describes staff-related requirements, focusing in particular on the role of Risk Manager. This part is based on ON Rule *ONR 49003*.

Part C
Part C addresses all requirements associated with the organizational structure of companies, focusing in particular on the requirement that a company's organizational structure must facilitate the smooth implementation of a risk management system (*ONR 49002-1*).

Part D
Part D addresses the special requirements involved in the risk assessment of new technologies with small knowledge base. It also describes the requirements governing risk identification (monitoring).

Part E
Part E addresses the requirements related to risk treatment, including, firstly, pro-active risk communication and, secondly, an issue management strategy. Part E of the certification standard is based to some extent on the VDI brochure *Risikokommunikation für Unternehmen (Risk reporting in companies)* and on ON Rule *ONR 49002-3*.

2 Risk Management System Requirements

2.1 General requirements

Basically, the requirements to be fulfilled by risk management systems are comparable, irrespective of the literature or standard on which the risk management system is based, and need only be aligned with the specific case in question. The general risk management system requirements which also apply to the CENARIOS® standard are outlined below. Specific requirements of the CENARIOS® standard which apply in addition to these general requirements are addressed in chapter 2.2.

Overall, a risk management process must cover the following stages:

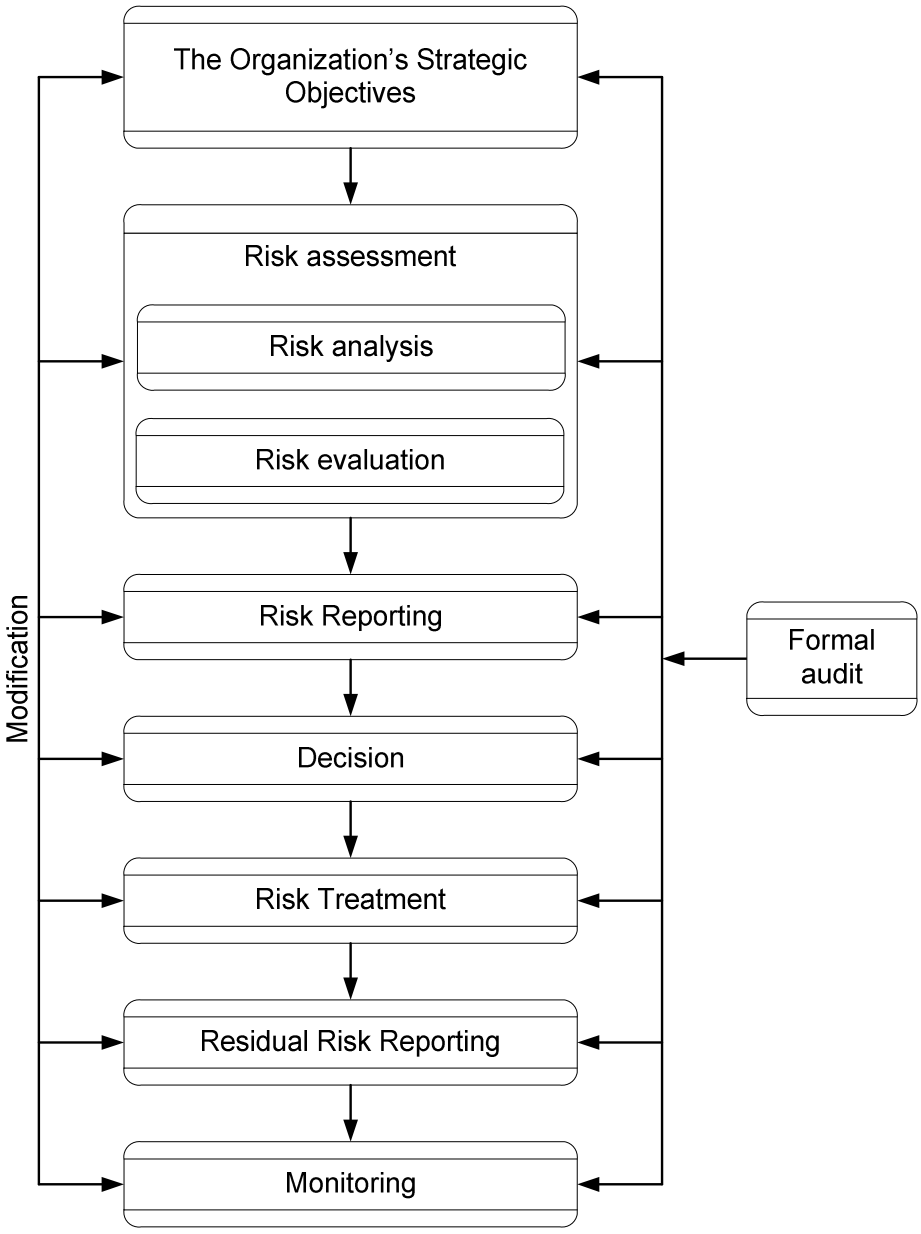

Figure 2-1 Risk management process, as illustrated in *A Risk Management Standard, FEDERATION OF EUROPEAN RISK MANAGEMENT ASSOCIATIONS (FERMA)*

The individual elements of a risk management process, including the formal audit, as shown in Figure 2-1 above, are described in detail in the above standard issued by FERMA. Section 2.3.4 includes a detailed flowchart aligned to the requirements of the CENARIOS® standard. The requirements of the CENARIOS® risk management standard pertaining to the six key elements shown in Figure 2-2 are described below.

Figure 2-2 Key modules of the CENARIOS® risk management system

2.1.1 Risk analysis

Risk analysis must provide answers to the following questions:

- What *events* may occur?
- How serious are the potential *consequences* of these events?
- What are the *root causes* underlying these events?
- What is the *probability* or *frequency of occurrence* of these events?

These parameters can be determined with the help of several qualitative, quantitative or semi-quantitative methods. The method best suited to the application in question should be selected depending on the level of knowledge and the analysis criteria.

2.1.2 Risk assessment

To assess the identified risks, the risks must be examined to determine whether they are acceptable or not. Numerical values indicating acceptance limits have been defined, in particular, in English-speaking countries, in the Netherlands and in Switzerland.

As there are no binding international rules defining what risk is acceptable and what risk is not, the ALARP (As Low As Reasonably Practicable) principle is recommended. The ALARP principle ensures that risks are only accepted after implementation of all feasible and, at the same time reasonable, risk reduction measures.

The planning of these measures must be an integral part of every risk management system.

2.1.3 Risk reduction

The risk management system must include measures which

- reduce the *probability or frequency of occurrence* and/or
- reduce the *consequences* of an event.

The approach selected for this purpose must be logical and outlined in the pertinent documentation. The assumed effectiveness of the measures taken must, in particular, be documented and verifiable.

As a matter of principle, a risk management system should always aim to reduce risks to the level defined in chapter 2.1.2 and thus pursue the planning and implementation of risk reduction measures.

Failure to achieve this goal must be documented. If the risk is accepted nevertheless, the reasons for this decision must be provided. Alternatively, further risk reduction measures must be taken (even if this ultimately results in the discontinuation of a product or product line).

2.1.4 Risk control

Changes in the operational processes for which the risk management system has been developed must be incorporated into the risk management system at regular intervals and the risks re-assessed.

These changes may vary to a great extent and may include necessary construction measures, introduction of a new supplier for individual products or recruitment of new employees.

2.1.5 Risk monitoring

Apart from changes in business operations, there may also be changes in the company's environment which necessitate risk re-assessment.

Changes in the field of science and technology may have considerable impacts on risk assessment.

A risk management system must include risk monitoring which identifies these changes at an early stage and allows measures to be taken.

Risk monitoring aims to identify changes in the environment which may influence the assessed risks at an early stage, re-assess these risks and take countermeasures, if necessary.

2.1.6 Risk treatment

All requirements outlined in chapters 2.1.1 to 2.1.5 notwithstanding, a company's image may suffer as a result of an event, or the company may be challenged directly with considerable or even existence threatening risks.

The risk management system thus must, firstly, verify that the company takes appropriate risk prevention measures and, secondly, provide systems to ensure risk treatment (e.g. crisis management, documented risk communication procedure).

2.2 Special requirements of the CENARIOS® standard

Basically, a risk management system in line with the CENARIOS® standard should enable a company to manage risks in the fields of

- health, safety and the environment, and
- product liability

as far as possible and in a predictable manner. The selected approach must be suitable to cover the specifics of nanotechnology and provide objective assessment.

Given this, special requirements have been defined for the production, the marketing and sales and the use of nanotechnology products which specify or go beyond the requirements outlined in chapter 2.1. These special requirements are outlined below.

2.2.1 Risk analysis requirements

In cases involving conventional technologies with vast operational experience there is sufficient data available to determine the *probability* or *frequency of occurrence* and adequate experience concerning the *consequences* of an event. Regarding the probability or frequency of occurrence, the experience gathered with other technologies may be transferred to nanotechnology and the normal standard methods applied.

As far as the consequences of an event are concerned, however, little information is generally available for new technologies. In nanotechnology, for example, there is hardly any reliable data regarding how permanent exposure to nanoparticles will affect the human organism or the environment.

In light of the above, a risk management system for nanotechnology must define and/or suggest a strategy in which a state-of-the-art estimate replaces the “consequences“ variable. This semi-quantitative approach is a key element of CENARIOS®.

2.2.2 Monitoring system requirements

As the state of the art in science and technology plays a major role in nanotechnology, any monitoring system applied to this field must be capable of documenting the state of the art at regular intervals and making it available for risk re-assessment.

In view of the fact that the legal situation has not yet been clarified, a monitoring system in nanotechnology – in contrast to a monitoring system for conventional technologies in the regulated sector, for example – must also identify changes in this sector at an early stage and enable companies to respond to these changes.

2.2.3 Risk treatment requirements

As nanotechnology develops in an environment characterized by rapid changes, pro-active elements of risk treatment, such as risk communication, are needed: Indicators are used to identify problem areas at an early stage and appropriate measures derived to avoid crises altogether, reduce them or manage them professionally.

The CENARIOS® risk management system therefore must include

- risk communication, and
- crisis or issue management

schemes as integral elements of risk treatment. Crisis and issue management and risk communication must basically cover the following stages:

- upstream crisis communication to ensure a prompt and internally coordinated first response to any event triggering a crisis.
- communication during the crisis to initiate effective responses
- downstream crisis communication to enable de-escalation.

The risk communication scheme should take a pro-active approach to actively form the public opinion.

2.3 Company-related requirements

The formal criteria to be fulfilled by companies seeking certification according to the CENARIOS® standard are outlined below.

2.3.1 Scope of application of the risk management system

A risk management system may apply throughout a company, to individual subsidiaries or may also be restricted to individual production sites or product lines. The company must define in advance, to which units and areas the risk management system is intended to apply and must document this scope of application.

2.3.2 Integration of risk management into the corporate culture

The company's policies must clearly state that risk management is a key element of corporate culture. This statement must be reflected in the corporate policy statement and in corporate governance guidelines.

Definition of normative goals
As a matter of principle, the key normative goals must be defined before a risk management system is established. These normative goals are, at first, abstract objectives and requirements related to risk awareness, risk perception, risk appetite and risk-aware operation which are defined by corporate culture.

Consideration of organizational framework conditions
The CENARIOS® risk management system is basically designed to be a stand-alone system. Due to its risk assessment and risk monitoring requirements, above all, seamless integration into existing risk management systems without any interfaces is impossible. The necessary interfaces and the requirements resulting from this must be assessed and documented.

2.3.3 Organizational structure and responsibilities

The prerequisites to implement the organizational regulations defined by the company must be established. In detail, this means that the organizational structure must reflect the requirements of the business unit in question.

The organizational structure illustrated in Figure 2-3 is an example of the minimum requirements to be complied with by a production company.

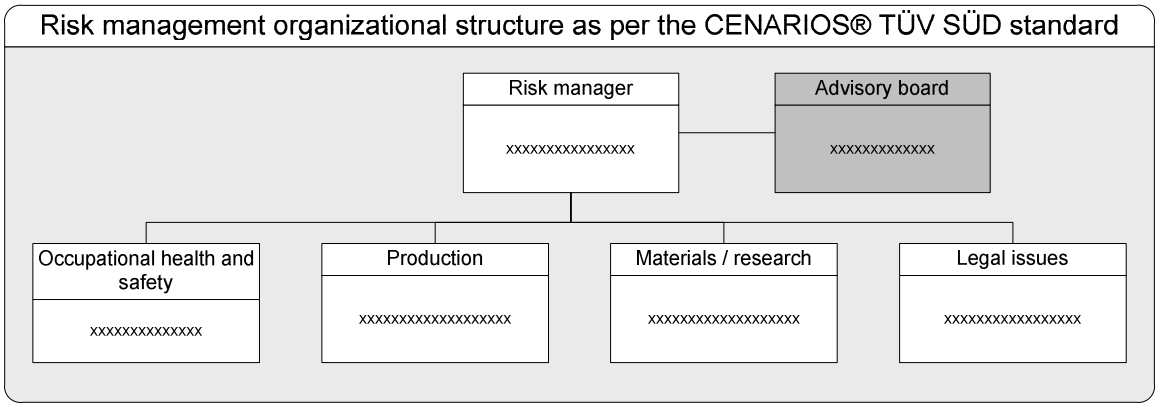

Figure 2-3 Proposed organizational structure of a risk management system

The white fields represent the key elements of the CENARIOS® risk management system which must be complied with by a company. Depending on the company's activities, these key elements may of course differ from the figure above, e.g. if a company does not produce nanomaterials but only places them on the market or sells them.

The elements and requirements described in the figure above may vary according to the size of the organization and range from a Risk Manager responsible for fulfilling all the above functions to a separate risk management unit.

Basically, deputies must be appointed for all individuals responsible for the above functions and regulations governing the transfer and delegation of tasks documented.

2.3.4 Documentation of the risk management process

The risk management process must be described in a document (e.g. a Risk Management Manual). The illustration of workflows in a flowchart has proved expedient for further implementation. Figure 2–4 is an example of such a flowchart. It illustrates the risk management process of a producer of nanomaterials and contains all key elements of risk assessment according to CENARIOS®.

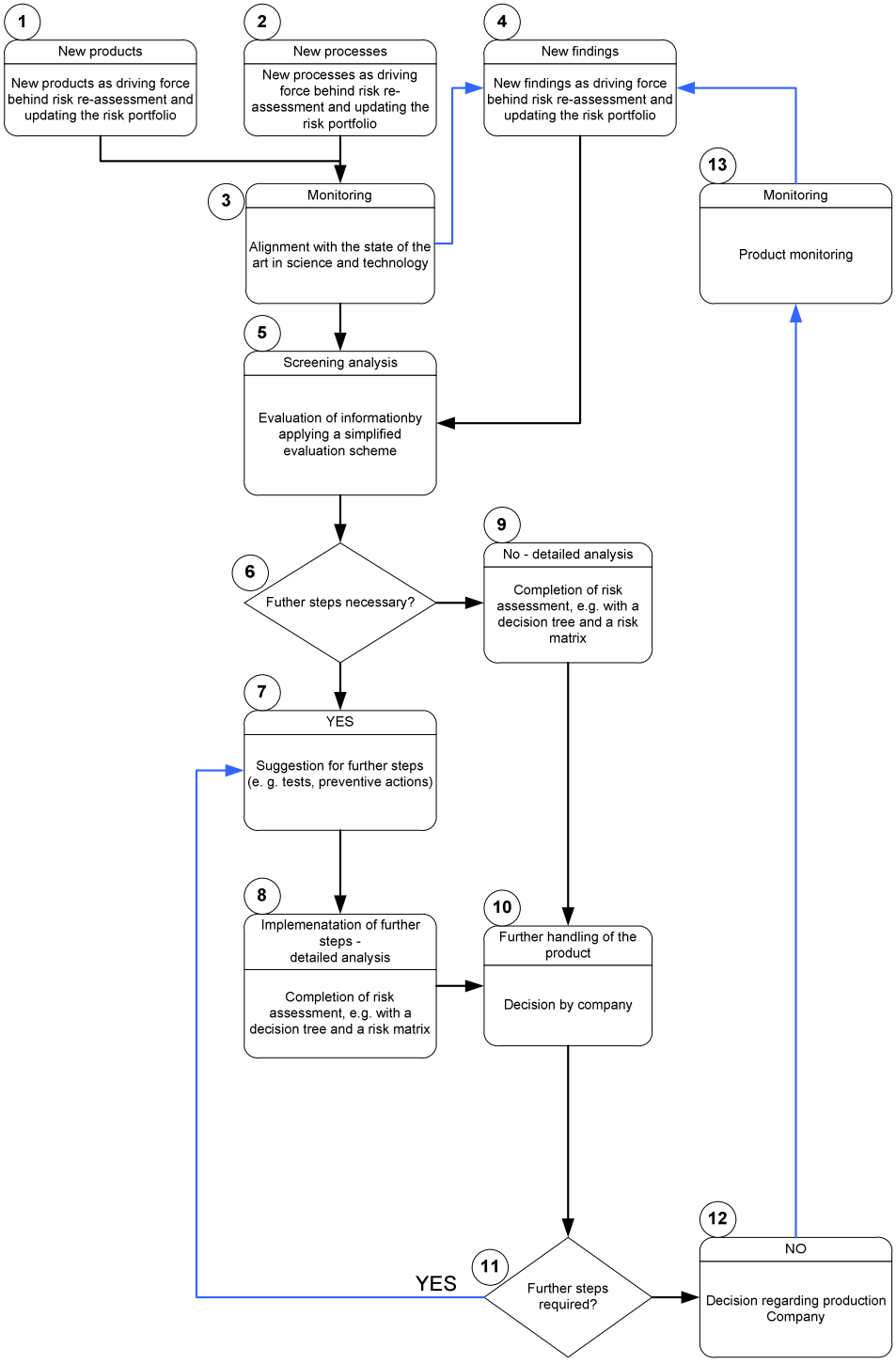

Figure 2-4 Example of a CENARIOS® risk management process

The 13 steps illustrated in figure 2–4 are explained in more detail below:

1. New products
   If the company plans to place a new product on the market, it must initiate the monitoring process for this product.
2. New processes
   The same applies if the company wishes to use new production processes.
3. Monitoring (state of the art in science and technology)
   The information in steps 1 and 2 must be subjected to monitoring. Monitoring reviews and describes the state of the art in science and technology for the products and/or processes defined in steps 1 and 2 above and defines the database applied to further assessment.
4. New findings
   Ongoing monitoring may supply new findings related to the products and/or processes defined in steps 1 and 2 above but also new findings which may be of interest for further risk assessment.
5. Screening analysis
   Based on the database defined in step 3 and further findings (e.g. expert knowledge available at the company which has not yet been published) assessment criteria must be defined. Building on these criteria, steps must be taken to ascertain whether the database is sufficient or whether additional information is needed to ensure the subsequent risk assessment is reliable. This information may be obtained through additional material testing. (To be seen in connection with the following step.)
6. Are further steps necessary?
   The result of this query follows directly from the previous process step.
7. Implementation of further steps
   If further steps (e.g. tests) are considered necessary in process steps 5 and 6, they will be carried out by suitable institutes or departments in order to expand the database.
8. Detailed analysis (including implementation of intermediate steps)
   Risk assessment is carried out on the basis of the database which may have been expanded by test results. In this context, the findings gained in process steps 5 to 7 are incorporated into a decision tree and define the path needed to determine the possible consequences of an event. After the probability or frequency of occurrence has been determined, the risk involved in various events can be mapped using the risk matrix and assigned to a risk category.
9. Detailed analysis (without implementation of intermediate steps)
   If process steps 5 and 6 do not necessitate further tests, risk assessment is effected based on the database as defined in process step 3 (monitoring). The approach is the same as in the previous process step.
10. Further handling of the product
    Based on the result obtained in risk assessment, the company decides on the further procedure.
11. Are further steps required?
    Similar to the results of process step 5, risk analysis (process step 9) may necessitate the initiation of further steps (material tests etc.). This applies, in particular, if the risk analysis reveals a high or unacceptable risk; in these cases process step 7 will be carried out next. Higher risks may also be accepted on a case-by-case basis, however. The decision rests with the company which must provide reasons for its decision, however.

12. Decision regarding production
    If no further tests are considered necessary in process step 11, the company may decide to start production based on the results of risk assessment.
13. Monitoring (product monitoring)
    Within the scope of risk management, every product should be monitored on an ongoing basis. If product monitoring leads to new findings, the process will start again at step 4.

2.3.5 Integration of risk management into existing quality management systems

The integration into already existing management systems must be defined and evidence of interfaces furnished.

If the company does not yet maintain any quality management systems into which the CENARIOS® system can be integrated or if the company plans to operate CENARIOS® as a stand-alone system right from the outset, all evidence must be furnished and documented explicitly for the system.

2.4 Requirements and the roles responsible for the individual functions

2.4.1 Risk Manager

The risk manager is responsible for implementing the results of the risk analysis and for establishing the risk management system or integrating it into already existing management systems.

2.4.2 Occupational Health and Safety Manager

The Occupational Health and Safety (OHS) Manager must ensure that all OHS requirements are complied with and must inform the Risk Manager of any risks that are not met by these requirements.

2.4.3 Production Manager(s)

Production Managers must ensure that all production processes including internal transport and storage are carried out in compliance with the generally accepted safety standards and do not involve any unnecessary risks. They must also inform themselves about the state of the art in production installations and modernize them, if necessary.

2.4.4 Materials/Research Manager

Materials/Research Managers must monitor educts, intermediate products, if any, and final products for non-conformities which may damage property or adversely affect health. They must be informed about the properties of starting materials. This information must be provided by the external suppliers of these materials (e.g. by means of material safety data sheets (MSDS)). In this context, the state of the art in science and technology must be applied in each case.

2.4.5 Legal Issue Manager

To regulate possible legal problems either pro-actively or because of a current event, the company must have a Manager which acts as contact in the event of legal issues.

2.4.6 Advisory Board

The company to be certified need not fulfil all key elements of the risk management system itself. This applies in particular to legal issues which may be delegated to competent and authorized individuals. With respect to materials and research it may also be sufficient to furnish evidence of cooperation with competent individuals or a research institute, for example.

Only the role of Risk Manager must be fulfilled inhouse, e.g. by an employee of the company in question. The responsibility for implementation of the risk management system must rest with the company to be certified while the implementation itself may be delegated to a person or institution represented on the Advisory Board.

Steps must be taken to ensure in all cases that the employees commissioned to fulfil roles within the scope of the risk management system are actually able and qualified to do so. Proof of their technical skills must be provided by furnishing evidence of appropriate technical qualifications. Additionally, steps must be taken to ensure that the qualifications of the individuals responsible for these roles are always up to date and correspond with the state of the art and that the responsible individuals also have the required soft skills (social skills, attitudes, ethics etc.).

2.5 Handling of risk management system

To keep the risk management system aligned with the state of the art in science and technology, a procedure must be established and documented which reliably identifies and implements changes in the state of the art in science and technology. The requirements associated therewith are specified in Section 2.1.5.

2.6 Verification of risk management system implementation

The professional implementation and maintenance of the risk management system must be verified in annual audits. This procedure must be an integral part of the risk management system. In these third-party audits (carried out by organizations independent of the company to be certified), the operator of the risk management system demonstrates compliance with the requirements outlined above, e.g. by means of its documented decision-making process.

2.7 Documentation requirements

Management system implementation and/or evidence to be submitted to the auditor requires a minimum of documentation. The contents and objectives of the documents needed are outlined below.

- Evidence of staff qualifications
  Evidence must be furnished that staff is able and qualified to fulfil their respective roles. For the Risk Manager, in particular, this includes evidence of completed education and training as well as of previous work experience. In other cases, evidence of regular follow-up training must be furnished in addition. This applies in particular to the Occupational Health and Safety managers.
- Systematic approach to risk identification and assessment.
  The process of risk identification and assessment must be documented in a comprehensible and traceable manner. In this context, special focus must be placed on the required semi-quantitative approach.

- Current risk inventory
  Risk assessment must be available for every current nanotechnology product. This risk assessment must, in particular, take into account the latest findings in risk monitoring. If monitoring does not lead to changes in risk assessment, a confirmation on the document ("document approved") will be sufficient.
- Knowledge base – history of risk assessment
  To be prepared for any inquiries or liability claims that may arise at a later stage, tracking of the current knowledge base must be possible for a minimum period of 10 years (in line with REACH requirements). Traceability also applies to the staff employed, risk monitoring results and the assessment of individual risks (see also "Current risk inventory").
- Crisis and issue management
  The response taken in the case of a foreseeable or existing crisis must be described in a comprehensible and traceable manner. In addition, crisis and issue management must ensure end-to-end documentation of adverse events. "Adverse events" include accidents affecting own and external staff as well as third parties (e.g. visitors). Events in production, e.g. inadequate batch quality/safety which may result in the destruction and/or non-delivery of this batch, must also be documented.
- Documentation of monitoring results
  Monitoring must be carried out on an ongoing basis. Monitoring results are used as the basis of risk assessment and must therefore, similar to the risk survey, be retained for a minimum period of 10 years.
- Strategy for implementing the risk management system as part of the corporate structure
  The company must maintain a documented strategy outlining how the risk management system is implemented in the company. The strategy may either describe how the individual modules are integrated into the existing quality management systems or specify how the overall scheme of the CENARIOS® standard is implemented as a stand-alone system.
- Instructions at workplaces and safety instructions
  Instructions which point out hazards and possible accident risks and include key emergency numbers must be available at all workplaces. These instructions must comply with the valid national guidelines of the institutions for the statutory accident insurance and prevention (Berufsgenossenschaften in Germany).

3 Certificate validity

The certificate will be valid for one year. After this period, the company must be re-certified. Otherwise it is no longer permitted to use the certificate. The certificate also becomes invalid if it is used for other than the agreed purposes or business areas.

The certification mark may only be used in connection with the certificate, i.e. it may be included on company brochures which, for advertising purposes, refer to the fact that the company's risk management system has been certified. Use of the certification mark alone, e.g. on products, is not permitted, however.

4 Bibliography

ONR 49000 Risk Management for Organizations and Systems – Terms and basics – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49001 Risk management for organizations and systems – Risk Management – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49002-1 Risk management for organizations and systems – Part 1: Guidelines for embedding the risk management in the management system Practical use of ISO/DIS 31000; 2008-06-01

ONR 49002-2 Risk management for organizations and systems – Part 2: Guideline for methodologies in risk assessment – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49002-3 Risk management for organizations and systems – Part 3: Guidelines for emergency, crisis and business continuity management – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49003 Risk management for organizations and systems – Requirements for the qualifications of the Risk Manager – Practical use of ISO/DIS 31000; 2008-06-01

FERMA A Risk Management Standard, published by AIRMIC, ALARM, IRM: 2002

VDI Risikokommunikation für Unternehmen (ISBN 3-931384-33-0).

Industrie Service

Choose certainty.
Add value.

CENARIOS® Certification Standard
Part B

Staff-Related Requirements

Date: 13 August 2008

Our references:
IS-ATC1-MUC

Document:
08-08-13 CENARIOS Certification Standard Part B.doc

This document consists of
8 pages
Page 1 of 8

Headquarters: Munich
Trade Register: Munich HRB 96 869

Supervisory Board:
Dr.-Ing. Axel Stepken (Chairman)
Board of Management:
Dr. Peter Langer (Spokesman)
Dipl.-Ing. (FH) Ferdinand Neuwieser

Telefon: +49 89 5791-0
Telefax: +49 89 5791-2888
www.tuev-sued.de

TÜV SÜD Industrie Service GmbH
Niederlassung München
Bereich Anlagentechnik
Westendstraße 199
80686 München
Deutschland

Industrie Service

Table of Contents

0 Preambel

This part B of the CENARIOS® certification standard[1] for risk management systems describes the staff-related requirements and focuses on the position of risk manager. The requirements to be satisfied by a Risk Manager have been taken from the ONR Rule *ONR 49003: Risk Management for Organisations and Systems – Requirements for the Qualifications of a Risk* Manager and aligned to the terms and conditions of the CENARIOS® standard.

In addition to the requirements that must be satisfied by the Risk Manager, the system also defines the criteria to be fulfilled by Occupational Health and Safety Managers, Production Managers, Materials/Research Managers and the Legal Issues Managers. Hereinafter, the individuals in charge of these roles are referred to as risk owners.

0.1 Other applicable documents

These staff-related requirements make up part 2 of the CENARIOS® certification standard for risk management systems which consists of a total of five parts. Part A of the CENARIOS® certification standard provides companies seeking to be certified with the preliminary information required in order to prepare for the certification process. Parts B to E of this standard contain more detailed information about the subjects addressed and aim to help companies to identify opportunities for improvement, if any.

Part A
Part A describes the general criteria and provides a summary of all subsequent parts of the standard. This part of the certification standard is based to some extent on *A Risk Management Standard* (FERMA).

Part B
Part B describes staff-related requirements, focusing in particular on the role of Risk Manager. This part is based on ON Rule *ONR 49003*.

Part C
Part C addresses all requirements associated with the organizational structure of companies, focusing in particular on the requirement that a company's organizational structure must facilitate the smooth implementation of a risk management system (*ONR 49002-1*).

Part D
Part D addresses the special requirements involved in the risk assessment of new technologies with small knowledge base. It also describes the requirements governing risk identification (monitoring).

Part E
Part E addresses the requirements related to risk treatment, including, firstly, pro-active risk communication and, secondly, an issue management strategy. Part E of the certification standard is based to some extent on the VDI brochure *Risikokommunikation für Unternehmen (Risk reporting in companies)* and on ON Rule *ONR 49002-3*.

[1] CENARIOS® is the legally protected name of the risk management system developed jointly by TÜV SÜD and Innovationsgesellschaft, St. Gallen, Switzerland.

1 Requirements to be satisfied by Risk Managers

1.1 Qualifications

Risk Managers of companies which operate in innovative fields of technology with little knowledge about the relevant risks, such as nanotechnology, must be able to identify, describe and document risks in the following areas

- health, safety and environment,
- product liability, and
- risks arising for manufacturers due to changes in legislation.

1.2 Qualification criteria

1.2.1 Knowledge of the terms and principles of risk management (ONR 49000)

Risk Managers must

- demonstrate the objective and purpose of risk management and convince risk owners that risk management is critical and useful for the organization and the system,
- correctly use and define risk management terms,
- describe the risk management scheme as part of the management system,
- appropriately define the scope of application of the risk management system regarding the organizational structure and with respect to systems, products, services, projects etc. and their relevant types of risks,
- known other risk analysis techniques, such as FMEA, fault tree and impact analysis, HAZOP and HACCP and must be able to assess when to apply what method and how this method must be used to develop and describe the risk portfolio in the risk landscape,
- be familiar with the interactions between risk management and other management tools and must be able to identify the interfaces depending on the situation in question.

1.2.2 General duties

Risk Managers must

- ensure, on behalf of top management, that the risk management process is introduced and a risk management system is established, operated and maintained,
- report to top management with regard to the performance of the risk management system and any improvements that may be needed;
- ensure risk awareness throughout the organization.

1.2.3 Guidelines for risk management

Risk Managers must

- align risk management with the organization's corporate policy and risk policy and understand risk within the overall context of the objectives and strategies of the organization and its external requirements and expectations,
- define and distinguish the scope of risk management, prepare an appropriate hazard list for the audit and maintain this list as knowledge base,
- define the criteria for the risk landscape (frequency/probability, consequences),

- determine risk scenarios jointly with the risk owners,
- carry out risk assessment jointly with the risk owners,
- quantify the costs and benefits involved in risk management,
- demonstrate the limits and areas of risk tolerance and, in conjunction with the risk owners, prepare a risk-benefit analysis (choice between conflicting rights),
- document risk management and/or the results of risk assessment.

1.2.4 Guidelines for embedding risk management into the management system

Risk Managers must

- expertly handle every step along the risk management process,
- position the risk management process in the process landscape of the organization,
- describe risk management applications by means of other processes and must demonstrate and document the interactions between the risk management process and other relevant processes;
- implement the results of risk assessment and maintain risk management;
- maintain and continuously improve the risk management system and all its elements.

1.2.5 Moderation and communication

Risk Managers must moderate risk management workshops and communicate convincingly with risk owners and colleagues on risk-related issues.

1.3 Advanced training

Risk Managers must participate in on-going advanced training to ensure their qualifications, as outlined under Section 1.2 hereunder, comply with the state of the art.

1.4 Transfer of tasks

Risk Managers may delegate definite tasks related to the operation of the CENARIOS® Risk Management System fully or partially to third parties (Advisory Board). The responsibility for decisions related to the risk management system cannot be delegated.

1.5 Deputy

The Risk Manager must appoint a deputy, who will fulfil the key tasks of the Risk Manager in the latter's absence.

1.6 Delegation of tasks

As a matter of principle suitable individuals must be appointed in each field of activity who must ensure that the results of risk analysis and risk evaluation will be implemented in their areas. The area-specific requirement profiles are described in the sections below.

2 Requirements for Occupational Health and Safety Managers and Experts

Occupational Health and Safety (OHS) Managers must ensure compliance with all OHS requirements and must inform the Risk Manager of any non-conformity in this area.

OHS Managers may consult an OHS expert or fulfil the function of OHS experts themselves.

In addition, OHS Managers must furnish evidence that they inform themselves at regular intervals about the possible risks in this technical area and must integrate this new information into their daily work.

To fulfil their role properly, OHS experts must have qualified technical expertise and methodological skills, must be able to conduct unbiased analysis and think in alternatives and must be capable of systematic thinking and approaches. Evidence of this knowledge and expertise must be furnished by attending regular advanced training courses on OHS. In the context of this standard, the OHS Manager must focus, in particular, on ensuring the implementation of specific protection measures.

Social skills such as assertiveness, interpersonal skills and tactfulness are also required. The OHS experts are to support the employer and/or the OHS Manager, i.e. they must in many cases cooperate directly with the OHS Manager and top management. They must also co-operate with all other individuals fulfilling roles or responsibilities in occupational health and safety management, such as supervisors, members of the staff association, company doctors and other officers and representatives. The role of OHS expert therefore requires a high level of initial qualifications.

It goes without saying that this role and these tasks can only be fulfilled effectively by individuals who are interested in this type of activity. OHS experts therefore should not be appointed against their will. OHS experts also need interpersonal skills which express themselves in attitudes, ethics, needs and motives.

3 Requirements for Production Managers

Production Managers must ensure that all production processes including internal transport and storage are carried out in compliance with the generally accepted safety standards and do not involve any unnecessary risks. They must also inform themselves about the state of the art in production installations and systems and must update them, if necessary.

Similar to OHS Managers, Production Managers also need social skills such as assertiveness, interpersonal skills and tactfulness. Production Managers must, firstly, cooperate with OHS Managers to ensure safe production and, secondly, be able to describe the requirements associated, for example, with impending modernization measures in such a plausible and conclusive manner that they convince the Risk Managers of the necessity of these measures.

The key tasks of Production Managers involve

- Planning, support and handling of orders
- Monitoring of production
- Management, development and training of production staff
- Continuous improvement of production processes
- Preventive maintenance of production facilities
- Co-operation with the occupational health and safety and quality management functions and the Risk Manager

Production Managers must be qualified to fulfil the above tasks on the basis of their education.

4 Requirements for Materials / Research Managers

Materials/Research Managers must monitor starting materials/educts, intermediate products, if any, and final products for non-conformities which may damage property or adversely affect health. They must be informed about the properties of starting materials supplied by external suppliers. This information must be provided by the external suppliers of these materials and must generally be described in material safety data sheets (MSDS). The evaluation of this information and of the details provided by the supplier must be based on the state of the art in science and technology.

The required information may be researched independently or in cooperation with the Advisory Board (see section 6).

These activities may even result in the recommendation to discontinue certain product lines and the responsibility for arguing this position against the Risk Manager and/or the decision makers in the company rests with the Material/Research Manager. Key abilities of Material/Research Managers in addition to technical qualifications therefore include in particular assertiveness and co-operativeness.

Evidence of technical qualifications must be furnished in the form of a scientific degree appropriate for the issues on hand and appropriate work experience. Evidence of regular attendance at materials/research events (in accordance with the focus of the company to be certified) must be furnished.

5 Requirements for Legal Issues Managers

To regulate possible legal issues either in a pro-active approach or because of a current incident, the company must have a contact person for legal issues. The legal disciplines of importance in nanotechnology should include product liability, the Chemicals Act and all legal disciplines associated therewith. Legal Issues Managers should be appropriately qualified.

6 Requirements for the Advisory Board

The company to be certified need not fulfil all key elements of the risk management system itself. This applies in particular to legal issues which may be delegated to competent and authorized individuals. With respect to materials and research it may also be sufficient to furnish evidence of cooperation with competent individuals or a research institute, for example.

Only the role of Risk Manager must be fulfilled inhouse, e.g. by an employee of the company seeking to be certified. The responsibility for implementation of the risk management system must rest with the company to be certified while the implementation itself may be delegated to a person or institution represented on the Advisory Board.

Depending on the tasks on hand, the requirements to be fulfilled by an Advisory Board which may be called in, where appropriate, correspond to the requirements defined in Sections 2 to 6 above.

7 Bibliography

ONR 49000 Risk Management for Organizations and Systems – Terms and basics – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49001 Risk management for organizations and systems – Risk Management – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49002-1 Risk management for organizations and systems – Part 1: Guidelines for embedding the risk management in the management system Practical use of ISO/DIS 31000; 2008-06-01

ONR 49002-2 Risk management for organizations and systems – Part 2: Guideline for methodologies in risk assessment – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49002-3 Risk management for organizations and systems – Part 3: Guidelines for emergency, crisis and business continuity management – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49003 Risk management for organizations and systems – Requirements for the qualifications of the Risk Manager – Practical use of ISO/DIS 31000; 2008-06-01

FERMA A Risk Management Standard, published by AIRMIC, ALARM, IRM: 2002

VDI Risikokommunikation für Unternehmen (ISBN 3-931384-33-0).

Industrie Service

Choose certainty.
Add value.

CENARIOS® Certification Standard
Part C

Organizational Requirements

Date: 13 August 2008

Our references:
IS-ATC1-MUC

Document:
08-08-13 CENARIOS Certification Standard Part C.doc

This document consists of
12 pages
Page 1 of 12

.

Headquarters: Munich
Trade Register: Munich HRB 96 869

Supervisory Board:
Dr.-Ing. Axel Stepken (Chairman)
Board of Management:
Dr. Peter Langer (Spokesman)
Dipl.-Ing. (FH) Ferdinand Neuwieser

Telefon: +49 89 5791-0
Telefax: +49 89 5791-2888
www.tuev-sued.de

TÜV®

TÜV SÜD Industrie Service GmbH
Niederlassung München
Bereich Anlagentechnik
Westendstraße 199
80686 München
Deutschland

Industrie Service

Table of Contents

0 Preamble

This part C of the CENARIOS® certification standard[1] for risk management systems describes the organizational requirements to be fulfilled by the company to be certified. The size of the company plays a major role in this context, so that there is a relatively high level of flexibility regarding the organizational requirements to be complied with for certification.

This flexibility may also refer, for example, to the form of the organizational structure. A small startup business, for example, may operate an effective risk management system as per the CENARIOS® standard without having to staff all the functions illustrated in Figure 1-1. The integration of the CENARIOS® risk management system into existing quality or risk management systems, which may prove reasonable but not mandatory for certification, also offers scope for interpretation.

0.1 Other applicable documents

These organizational requirements represent part three of the CENARIOS® standard for risk management systems which comprises five parts in total. Part A of the certification standard provides companies seeking to be certified with the preliminary information required in order to prepare for the certification process. Parts B to E of this standard contain more detailed information about the subjects addressed and aim to help companies to identify opportunities for improvement, if any.

Part A
Part A describes the general criteria and provides a summary of all subsequent parts of the standard. This part of the certification standard is based to some extent on *A Risk Management Standard* (FERMA).

Part B
Part B describes staff-related requirements, focusing in particular on the role of Risk Manager. This part is based on ON Rule *ONR 49003*.

Part C
Part C addresses all requirements associated with the organizational structure of companies, focusing in particular on the requirement that a company's organizational structure must facilitate the smooth implementation of a risk management system (*ONR 49002-1*).

Part D
Part D addresses the special requirements involved in the risk assessment of new technologies with small knowledge base. It also describes the requirements governing risk identification (monitoring).

Part E
Part E addresses the requirements related to risk treatment, including, firstly, pro-active risk communication and, secondly, an issue management strategy. Part E of the certification standard is based to some extent on the VDI brochure *Risikokommunikation für Unternehmen (Risk reporting in companies)* and on ON Rule *ONR 49002-3*.

[1] CENARIOS® is the legally protected name of the risk management system developed jointly by TÜV SÜD and Innovationsgesellschaft, St. Gallen, Switzerland.

1 Organizational requirements

The organizational requirements which companies must fulfil in order to be certified according to the CENARIOS® standard are outlined below.

1.1 Scope of application of the risk management system

A risk management system may apply throughout a company, to individual subsidiaries or may also be restricted to individual production sites or product lines. This basically also applies to the CENARIOS® risk management system. In larger companies, the use of nanotechnology will frequently be limited to certain business units or areas, which means the scope of the certification will be similarly limited.

In line with the above, companies seeking to be certified must define the

- business units and areas,
- production sites, and
- product lines

to which the risk management system will apply. This scope of application must be defined and documented in advance and forms the framework conditions for the further development and continuous improvement of the risk management system.

1.2 Integration of CENARIOS® into the corporate culture

The company's policies must clearly state that risk management is a key element of corporate culture. This statement must be reflected in the corporate policy statement and in corporate governance guidelines.

1.2.1 Definition of normative goals

As a matter of principle, the key normative goals must be defined before a risk management system is established. These normative goals are, initially, abstract objectives and requirements which will define the corporate culture in terms of risk awareness, risk perception, risk appetite and risk-aware operation.

For this purpose, answers to the following questions must be defined and documented:

- Why does the company plan to establish a risk management system?
- Within the scope of its possibilities, what risks is the company prepared to accept knowingly?
- What risks must not be accepted? The answer to this question must take the applicable laws, codes of practice and the state of the art into consideration.
- How can staff be given an understanding of these goals and objectives?

Answering these questions helps to identify and position the various risk areas described in Part D of this certification standard.

1.2.2 Consideration of organizational framework conditions

Basically, the CENARIOS® risk management system has been designed as a stand-alone system. Due to its risk assessment and risk monitoring requirements, above all, a seamless integration into existing risk management systems without any interfaces is impossible. Given this, the following aspects must be verified:

- Has the company defined requirements for the risk management system which apply throughout the entire company (e.g. acceptance limits which are defined by the amounts covered by insurance)?
- Are these requirements suitable for the CENARIOS® risk management system? I.e.:
  - Have the contacts named in Part B of this certification standard been integrated?
  - Does the risk assessment and risk monitoring scheme described in part D of this certification standard comply with the defined requirements?
  - Does the company maintain a scheme for risk treatment as outlined in part E of this standard?
- If the answer to the above question is no, the company must furnish evidence that it has interfaces which are suitable for the integration of the CENARIOS® risk management system (e.g. integration into an existing QM system or establishment as stand-alone system).

1.3 Definition of roles and responsibilities

The prerequisites for implementing the organizational regulations defined by the company must be established. In detail, this means that the organizational structure must reflect the requirements of the business unit in question.

The organizational structure illustrated in Figure 1-1 is an example of the minimum requirements to be complied with by a production company.

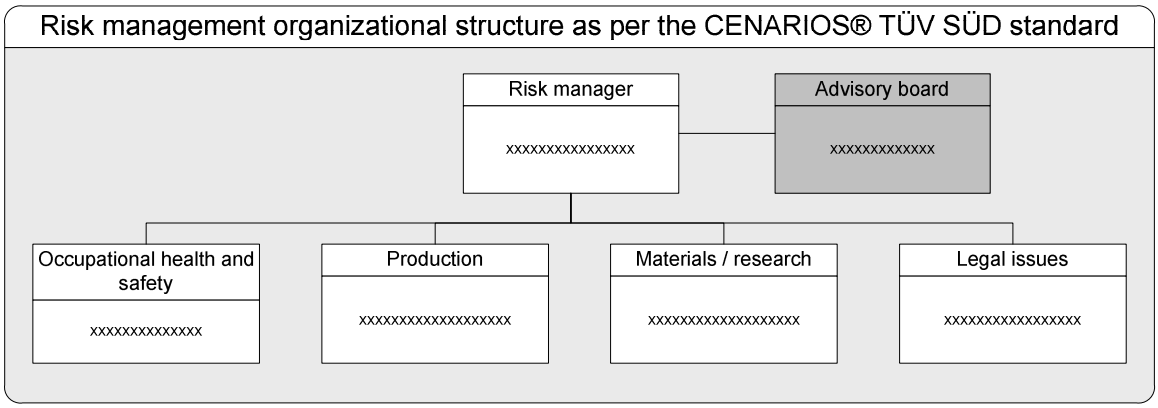

Figure 1-1 Proposed organizational structure for a risk management system

The white fields represent the key elements of the CENARIOS® risk management system which must be complied with by a company. Depending on the company's activities, these key elements may of course differ from the figure above, e.g. if a company does not produce nanomaterials but only places them on the market or sells them.

The requirements to be fulfilled by the individuals responsible for the individual fields in Figure 1-1 are outlined in *Part B – Staff-Related Requirements* of the certification standard.

The staff-related requirements described there may vary according to the size of the organization and range from a Risk Manager responsible for fulfilling all the above functions to an independent

risk management unit. The most common – and in many cases also most reasonable – variant is that the above functions are carried out by appropriately qualified experts within the scope of their normal activities.

All risk management systems as per the CENARIOS® standard must include issues and crisis management as well as risk communication, which are central elements of a risk management system (see part E of the certification standard).

The requirements associated with issues and crisis management and risk communication and/or their implementation within the company depend very much on the company's size. In a small company, for example, the Managing Director will assume the role of Risk Manager and also be responsible for risk communication, while very large companies will have their own corporate communications and public relations departments which largely function independently of the operating units (see figure 1-2).

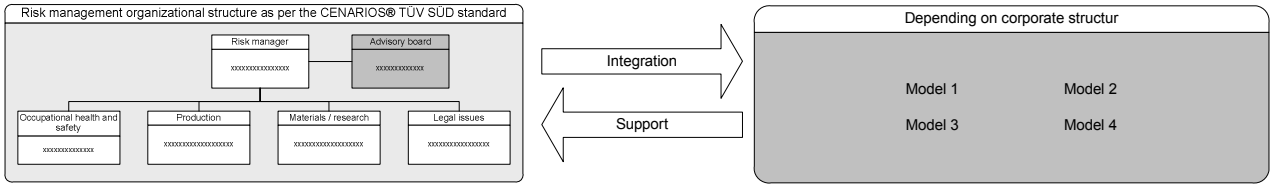

Figure 1-2 Integration of crisis/issue management
and/or risk communication into the risk management system

More detailed information about the integration of crisis management and risk communication into the company is included in part E of this standard.

2 Implementation-related requirements

2.1 Documentation of the risk management process

The risk management process must be described in a document, for example a Risk Management Manual. The illustration of workflows in an appropriate way has proved necessary for further implementation. The flowchart in Figure 2-1 is an example and includes all key elements of risk assessment in line with the CENARIOS® standard.

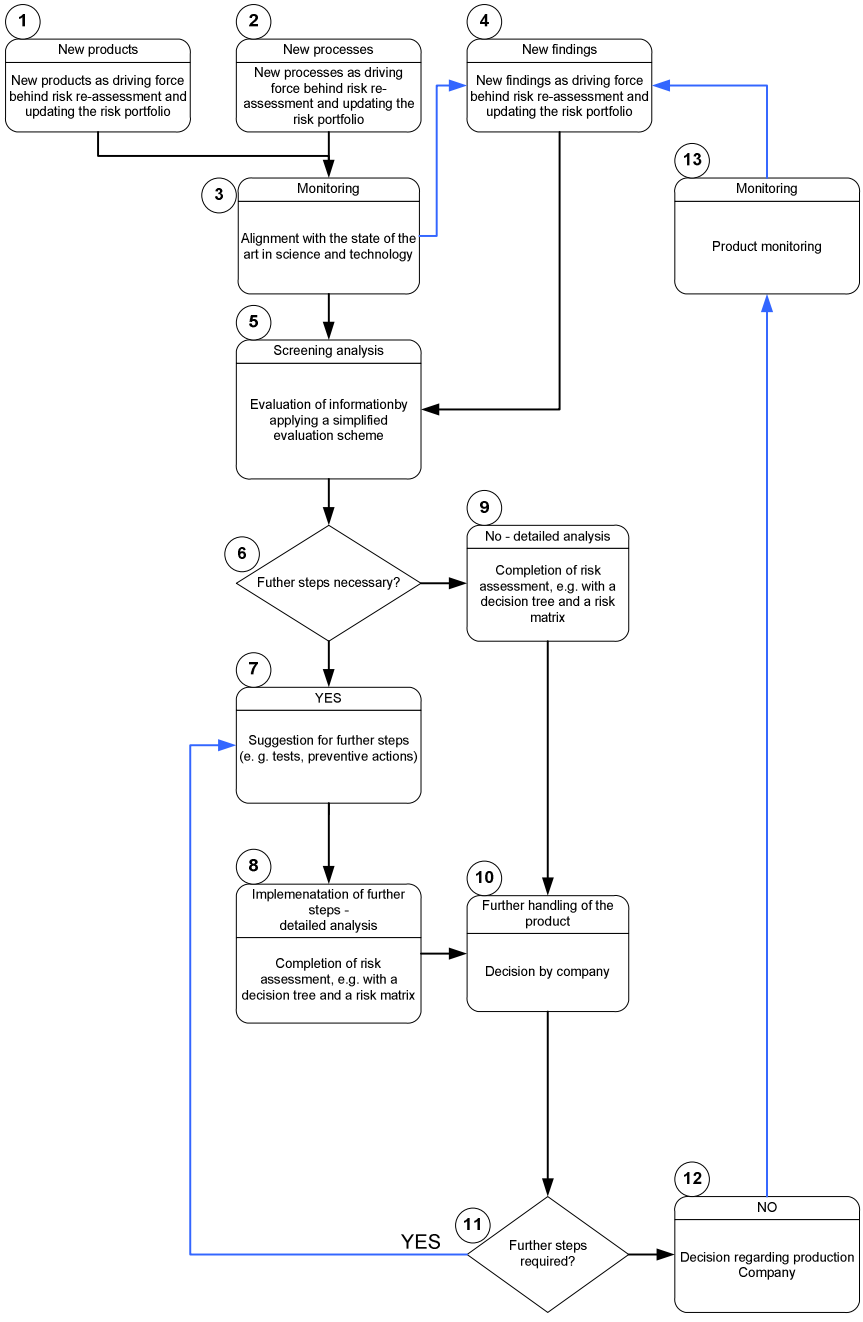

Figure 2-1 Example of a CENARIOS® risk management process

The above flowchart illustrates the interactions of the complete risk assessment and risk monitoring processes.

To integrate the system into an existing quality management system, e.g. as per ISO 9000/9001, dividing the process shown in figure 2-1 into different sub-processes has proved meaningful and/or necessary.

2.1.1 Explanation of the approach

The 13 steps illustrated in figure 2-1 are described in detail below:

1. New products
   If the company plans to place a new product on the market, it must initiate the monitoring process for this product.
2. New processes
   The same applies if the company wishes to use new production processes.
3. Monitoring (state of the art in science and technology)
   The information in steps 1 and 2 must be subjected to monitoring. Monitoring reviews and describes the state of the art in science and technology for the products and/or processes defined in steps 1 and 2 above and defines the database applied to further assessment.
4. New findings
   Ongoing monitoring may supply new findings related to the products and/or processes defined in steps 1 and 2 above but also new findings which may be of interest for further risk assessment.
5. Screening analysis
   Based on the database defined within the scope of step “monitoring (state of the art in science and technology)” and further findings (e.g. expert knowledge available at the company which has not yet been published) assessment criteria must be defined. Building on these criteria, steps must be taken to ascertain whether the database is sufficient or whether additional information is needed to ensure the subsequent risk assessment is reliable. This information may be obtained through additional material testing. (To be seen in connection with the following step.)
6. Are further steps required?
   The result of this query follows directly from the previous process step.
7. Implementation of further steps
   If further steps (e.g. tests) are considered necessary in process steps 5 and 6, they will be carried out by suitable institutes in order to expand the database.
8. Detailed analysis (including implementation of intermediate steps)
   Risk assessment is carried out on the basis of the database which has been expanded by test results. In this context, the findings gained in process steps 5 to 7 are incorporated into a decision tree and define the path needed to determine the possible consequences of an event. After the probability or frequency of occurrence has been determined, the risk involved in various events can be mapped using the risk matrix and assigned to a risk category.
9. Detailed analysis (without implementation of intermediate steps)
   If process steps 5 and 6 do not necessitate further tests, risk assessment is effected based on the database as defined in process step 3 (monitoring). The approach is the same as in the previous process step.

10. Further handling of the product
    Based on the result obtained in risk assessment, the company decides on the further procedure.
11. Are further steps required?
    Similar to the results of process step 5, risk analysis (process step 9) may necessitate the initiation of further steps (material tests etc.). This applies, in particular, if the risk analysis reveals a high or unacceptable risk; in these cases process step 7 will be carried out next. Higher risks may also be accepted on a case-by-case basis, however. The decision rests with the company which must provide reasons for its decision, however.
12. Decision regarding production
    If no further tests are considered necessary in process step 11, the company may decide to start production based on the results of risk assessment.
13. Monitoring (product monitoring)
    Within the scope of risk management, every product should be monitored on an ongoing basis. If product monitoring leads to new findings, the process will start again at step 4.

2.2 Integration of the risk management system into existing quality management systems

The following interfaces exist between risk management systems as per the CENARIOS® standard and other management systems, e.g. as per ISO 9001, ISO/TS 16949, ISO 14001:

- Management responsibility (requirements for Risk Manager)
- Resource management (staff-related requirements),
- (Risk management) process (Part D of the certification standard),
- System monitoring (Part D and/or E of the certification standard).

For certification, companies must furnish proof of the interfaces of the risk management system with the above quality management systems and/or of the integration of the CENARIOS® risk management system into existing quality management systems.

2.3 Operation of the CENARIOS® risk management system as stand-alone system

If the company does not yet maintain any quality management systems into which the CENARIOS® system can be integrated or if the company plans to operate CENARIOS® as a stand-alone system right from the outset, all evidence must be furnished explicitly for the system. The documentation required for this purpose is described in the following Section.

3 Documentation requirements

Management system implementation and/or evidence to be submitted to the auditor require a certain minimum of documentation. The contents and objectives of the documents needed are outlined below.

- Evidence of staff qualifications
  Evidence must be furnished that staff is able and qualified to fulfil their respective roles. For the Risk Manager, in particular, this includes evidence of completed education and training as well as of previous work experience. In other cases, additional evidence of regularly attended advanced training courses will be required. The same applies to the nanotechnology sector and here, in particular to Occupational Health and Safety Managers.

- Systematic approach to risk identification and assessment.
  The process of risk identification and assessment must be documented in a comprehensible and traceable manner. Special focus in this context must be on the semi-quantitative approach described in Part D of the certification standard.

- Current risk survey
  Risk assessment must be available for every current product which is a nanomaterial or in which a nanomaterial has been used for a specific purpose. This risk assessment must, in particular, take into account the latest findings in risk monitoring. If monitoring does not lead to changes in risk assessment, a confirmation on the document ("document approved") will be sufficient.

- Knowledge base – history of risk assessment
  To be prepared for any inquiries or liability claims that may arise at a later stage, tracking of the current knowledge base must be possible for a minimum period of 10 years (in line with REACH requirements). Traceability also applies to the staff employed, risk monitoring results and the assessment of individual risks (see also "Current risk survey").

- Issues and crisis management
  The response taken in the case of a foreseeable or existing crisis must be described in a comprehensible and traceable manner. More in-depth information about the detailed requirements is included in Part E of this certification standard. In addition, issues and crisis management must ensure end-to-end documentation of adverse events. "Adverse events" include but are not limited to accidents affecting own and external staff as well as third parties (e.g. visitors). Events in production, e.g. inadequate batch quality/safety which may result in the destruction and/or non-delivery of this batch, must also be documented.

- Documentation of the monitoring results
  Monitoring must be carried out on an ongoing basis and must verify that the company regularly reviews (a) suitable database(s) for the latest findings and changes in the level of knowledge concerning the impacts on human toxicology and ecotoxicology of the nanomaterials produced by the company or processed in other products of the company. Where appropriate, these findings must be incorporated into the research, design and development, and production activities in the company. The results must be updated at regular intervals, as a minimum requirement every three-months. Monitoring results are used as the basis of risk assessment and must therefore, similar to the risk survey, be retained for a minimum period of 10 years.

- Strategy for implementing the risk management system as part of the corporate structure
  The company must maintain a documented strategy outlining how the risk management system is implemented in the company. The strategy may either describe how the individual modules are integrated into the existing quality management systems or specify how the overall scheme of the CENARIOS® risk management is implemented as a stand-alone system.
- Instructions at workplaces and safety instructions
  Instructions which point out hazards and possible accident risks and include key emergency numbers must be available at all workplaces. These instructions must comply with the valid national guidelines of the institutions for the statutory accident insurance and prevention (Berufsgenossenschaften in Germany). Information about the type and scope of these instructions are included, e.g., in the “Guidance for handling and use of nanomaterials at the workplace“ published by the Federal German Institute for Occupational Safety and Health (Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, BAuA). If necessary, additional findings gained in risk assessment should be included in these instructions.

4 Bibliography

ONR 49000 Risk Management for Organizations and Systems – Terms and basics – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49001 Risk management for organizations and systems – Risk Management – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49002-1 Risk management for organizations and systems – Part 1: Guidelines for embedding the risk management in the management system Practical use of ISO/DIS 31000; 2008-06-01

ONR 49002-2 Risk management for organizations and systems – Part 2: Guideline for methodologies in risk assessment – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49002-3 Risk management for organizations and systems – Part 3: Guidelines for emergency, crisis and business continuity management – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49003 Risk management for organizations and systems – Requirements for the qualifications of the Risk Manager – Practical use of ISO/DIS 31000; 2008-06-01

FERMA A Risk Management Standard, published by AIRMIC, ALARM, IRM: 2002

VDI Risikokommunikation für Unternehmen (ISBN 3-931384-33-0).

Industrie Service

Choose certainty.
Add value.

CENARIOS® Certification Standard
Part D

Risk assessment and monitoring requirements

Date: 13 August 2008

Our reference:
IS-ATC1-MUC

Document:
08-08-13 CENARIOS Certification Standard Part D.doc

This document consists of
13 pages
Page 1 of 13

.

Headquarters: Munich
Trade Register: Munich HRB 96 869

Supervisory Board:
Dr.-Ing. Axel Stepken (Chairman)
Board of Management:
Dr. Peter Langer (Spokesman)
Dipl.-Ing. (FH) Ferdinand Neuwieser

Telefon: +49 89 5791-0
Telefax: +49 89 5791-2888
www.tuev-sued.de

TÜV®

TÜV SÜD Industrie Service GmbH
Niederlassung München
Bereich Anlagentechnik
Westendstraße 199
80686 München
Deutschland

Table of Contents

0 Preamble

This part D of the CENARIOS® certification standard[1] for risk management systems describes the requirements within the scope of risk assessment and monitoring. The special requirements applicable to risk management systems according to the CENARIOS® standard result to some extent from the currently low level of knowledge in the risk assessment of nanomaterials.

0.1 Other applicable documents

These risk assessment and monitoring requirements represent part four of the CENARIOS® standard for risk management systems which comprises five parts in total. Part A of the CENARIOS® certification standard provides companies seeking to be certified with the preliminary information required in order to prepare for the certification process. Parts B to E of this standard contain more detailed information about the subjects addressed and aim to help companies to identify opportunities for improvement, if any.

Part A
Part A describes the general criteria and provides a summary of all subsequent parts of the standard. This part of the certification standard is based to some extent on *A Risk Management Standard* (FERMA).

Part B
Part B describes staff-related requirements, focusing in particular on the role of Risk Manager. This part is based on ON Rule *ONR 49003*.

Part C
Part C addresses all requirements associated with the organizational structure of companies, focusing in particular on the requirement that a company's organizational structure must facilitate the smooth implementation of a risk management system (*ONR 49002-1*).

Part D
Part D addresses the special requirements involved in the risk assessment of new technologies with small knowledge base. It also describes the requirements governing risk identification (monitoring).

Part E
Part E addresses the requirements related to risk treatment, including, firstly, pro-active risk communication and, secondly, an issue management strategy. Part E of the certification standard is based to some extent on the VDI brochure *Risikokommunikation für Unternehmen (Risk reporting in companies)* and on ON Rule *ONR 49002-3*.

[1] CENARIOS® is the legally protected name of the risk management system developed jointly by TÜV SÜD and Innovationsgesellschaft, St. Gallen, Switzerland.

1 Risk Assessment Requirements

For the purpose of this standard, risk is defined in line with ISO/IEC Guides 51 and 73 which describe "risk" as a combination of the probability (frequency of occurrence) of an event and the consequences resulting from this. In mathematical terms, risk is often expressed as a multiplication of these two factors. While, in production processes, probability or frequency of occurrence is relatively easy to quantify, or at least estimate, it is generally known that the same cannot be said for consequences in nanotechnology.

It should be mentioned that this "technical" definition of risk is different from the "toxicological" risk: In medicine, "risk" is regarded more as a combination of hazard and exposure. In this context, the terms hazard and/or exposure used in the medical definition correspond roughly to the terms consequences and/or probability used in the technical definition. Unfortunately, however, there is no exact correspondence. This standard applies the technical definition of risk while acknowledging that different approaches may in fact be suitable and expedient in other contexts.

Risk analysis therefore must provide answers to the following questions:

- What *events* may occur?
- How serious are the potential *consequences* of these events?
- What are the *root causes* underlying these events?
- What is the *probability* or *frequency of occurrence* of these events?

These parameters can be determined with the help of several qualitative, quantitative or semi-quantitative methods. The method best suited to the application in question should be selected depending on the level of knowledge and the analysis criteria.

To assess the identified risks, the risks must be examined to determine whether they are acceptable or not. Numerical values indicating acceptance limits have been defined, in particular, in English-speaking countries, in the Netherlands and in Switzerland.

As there are no binding international rules defining what risk is acceptable and what risk is not, the ALARP (As Low As Reasonably Practicable) principle is recommended. The ALARP principle ensures that risks are only accepted after implementation of all feasible and, at the same time, reasonable risk reduction measures.

The planning of these measures must be an integral part of every risk management system.

2 The foundations of semi-quantitative risk assessment

So-called semi-quantitative methods are superior to purely quantitative methods, such as fault tree or event process analyses, in that they enable the consideration of both objective failure data and expert knowledge. In this context, it must be borne in mind that failure data frequently cannot be provided for specific cases, so that their order of magnitude can only be estimated anyhow. Semi-quantitative methods explicitly take this into account and allow subjective assessments to be linked to objective experience.

Risk assessment according to the CENARIOS® standard must, therefore, be based at least on a semi-quantitative approach. Qualitative risk assessment, e.g. in the form of a What-If-analysis or FMEA is not sufficient.

The identification of risks and risk-reduction measures must be based on events. This means that damage can only occur if an event caused by technical, human or organizational error(s) may cause injuries to people or damage to the environment. It is assumed that all of these cases involve concentrations harmful to people.

General risk analysis therefore must start by determining possible damaging events. In step 2, consequences must then be assigned to these events. In nanotechnology, consequences are generally the potential consequences which must be suitably estimated (Section 3).

Starting from the events, all sources or hazards which may trigger an event, down to the root causes, will then be identified. Probabilities or frequencies of occurrence must then be assigned to these root causes.

In nanotechnology, the inhalation of nanomaterials might be a possible event occurring during production, e. g. The hazard in this case could be pipe leakage while the root cause would be corrosion of the pipe.

The following action plan must assess the effectiveness of the protection levels which include preventive measures and safety-oriented functions in order to reduce risk probability and barriers to mitigate the consequences and assign them to the damage mechanisms identified in the risk analysis.

In the above example, the probability that nanomaterials are inhaled can be reduced by wearing suitable respiratory protection (barriers) and by installing sensors to detect pipe leakage (safety-oriented measure). In this case, preventive measures would involve the installation of suitable monitoring equipment, e.g. regular corrosion monitoring devices.

The probability of hazards and events is calculated semi-quantitatively on the basis of observed values of root causes and/or sources and hazards.

+Each damaging event is determined by probability and consequence. These events are entered in a risk matrix, as for example shown in Figure 2-1. The risk matrix uses discrete categories for probability (e.g. "1" to "5") and consequences (e.g. "A" to "E"). These parameters are estimated by means of a qualitative or semi-quantitative approach and then expressed in these discrete categories. Category "5" for example may stand for "almost certain", while "1" stands for "extremely unlikely". Similarly, "E" may stand for "severe" and "A" for "negligible" consequences. The next higher and next lower categories differ by approximately one order of magnitude in each case.

Risks falling in section I (green) are acceptable (see above under risk assessment). If a system is positioned in this sector, no further risk-reducing measures are required from the point of safety technology. For risks falling in section II (yellow and amber transition zone) improvement measures may prove meaningful, while for risks positioned in sector III (red) they are an absolute must.

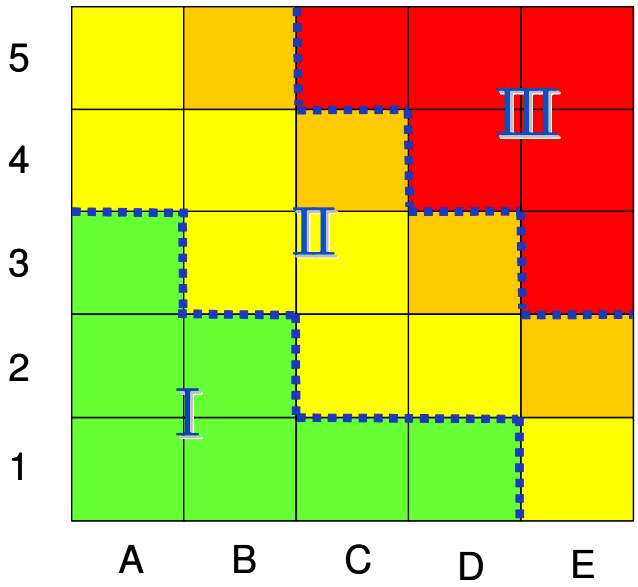

Figure 2-1 General risk matrix

As scaling and specifications take place before the assessment of individual events and measures, this approach, firstly, facilitates impartial and objective assessment and, secondly, ensures a high level of transparency of each individual assessment.

The positions of the damaging events in the risk matrix are determined by the results obtained in risk analysis (probability and consequence).

3 Special Requirements for Risk Analysis

Risk analysis requirements in innovative technologies differ clearly from those in conventional fields of technology. In most cases, there are hardly any experiences with or reliable knowledge of the probability and/or consequences of events in innovative technologies. The level of knowledge of the parameters required for risk identification is thus frequently inadequate.

3.1 Significance of the state of the art in science and technology

To overcome this difficulty and still be able to conduct a risk analysis, one must research the state of the art in science and technology and analyse the data collected against this state of the art. Knowledge management and/or monitoring are therefore key elements of risk analysis (see 4.). Depending on the level of knowledge, decisions can then be made on this basis which – depending on the company's risk appetite (see Part C of this certification standard) – involve a lower or higher risk for the company. The best possible research into the state of the art in science and technology at the time of decision making is crucial in this context.

3.2 Determining of possible consequences

Within the scope of risk management, grouping possible events into categories is sufficient to determine the *possible* consequences. This categorization does not replace individual product testing but forms the basis thereof and contributes significantly to minimizing the development risk.

For this purpose, the current level of knowledge must have been thoroughly researched, however, (see below) and be reliable enough to enable the determination of possible consequences. If this is not the case, either own toxicological analyses must be initiated[2], the hazardous material replaced by a material that has been better researched or the product in question not placed on the market for the time being.

The following table shows one example for the classification of possible consequences:

Category of potential consequences	Possible consequences arising from the handling of nanomaterials
Category A	No health impacts
Category B	Short-term minor health impacts of sensitive individuals
Category C	Short-term minor health impacts which will be avoided through compliance with safety regulations (e.g. feeling temporarily unwell)
Category D	Non-chronic health impacts which will be avoided through compliance with safety regulations and taking simple protective measures (e.g. skin lesions)
Category E	Chronic health impacts. Compliance with safety regulations, active protective measures and barriers are absolutely essential.
Category F	Severe chronic health impacts (e.g. genotoxicity, mutagenicity, lethal consequences). Compliance with safety regulations, active protective measures and barriers are absolutely essential.

Table 3-1 Categories for assessing the severity of possible consequences

[2] cf. for example NanoRisk Framework von Environmental Defense und DuPont

3.2.1 Stage 1: Database evaluation

Based on the state of the art in science and technology, the company must decide whether placing the nanomaterial or the product which contains the nanomaterial on the market

- is safe, so that production can be started, or
- is not safe enough and requires further scientific studies and examinations before production can be launched.

The safety-related criterion on which this decision should be based is whether health and/or environmental impacts have been adequately analyzed and examined. For this purpose, the knowledge published throughout the world must be reviewed and the relevant[3] publications identified.

The required level of due care must be applied to the estimation of the state of the art in science and technology. The survey must ensure that

- all available relevant sources of information have been identified and recorded in as much detail as possible
- a systematic and substantiated approach is applied to the selection and analysis of information sources
- it is continued on an ongoing basis and reliably reflects the current state of the art in science and technology at all times.

The identification of the state of the art in science and technology is based on monitoring which is described in Section 4.

3.2.2 Stage 2: Applicability of information sources

The information sources researched as outlined in Section 3.2.1 above must be evaluated. In this context, "evaluation" means that the publications are reviewed to ensure their contents are applicable to the case in question and their data sources (e.g. journal reputation) and authors reliable. The approach may be oriented to recognized standards (cf. e.g. U.S. Environmental Protection Agency: 2003) and must enable the required differentiated evaluation of data quality) The following criteria should be used for classification:

1. Transferable findings
   Can findings be generalized and transferred to humans? To verify this point, one determines whether data has been obtained by means of theoretical calculations or simulations or empirically by means of in vitro or in vivo testing on animal or human models.
2. Consistent findings
   How do the findings offered by the information source match the already existing knowledge? The information source must be evaluated to see whether findings are consistent and coherent or whether scientific and technological findings are conflicting.
3. Reliable information source
   What is the quality of the information source? To answer this question, the expertise and reputation of the identified sources of information must be assessed.

[3] "Relevant" in this case means that publications should be (publicly) available, should provide a sufficiently accurate specification of the nanomaterial used by the manufacturer or should be transferable to it and should enable conclusions with respect to toxicological outcomes. Information which is not publicly available (e.g. internal research results) may also be used.

3.3 Determining the probability of events

The categories of probability must be selected similar to standard risk assessment. In the case of nanotechnology, the probability of the events under review is either known from experience or must be substantiated. To do so, the company needs qualified event reports from the production processes in question and/or – where this proves impossible – qualified expert estimates. Estimates of probability, e.g. in line with the categories outlined in Table 3-2, must be documented comprehensibly and traceably.

Category of probability	Description
Category 1	Extremely unlikely $< 10^{-4}$ per year
Category 2	Unlikely 10^{-4} – 10^{-3} per year
Category 3	Rarely 10^{-3} – 10^{-2} per year
Category 4	Occasionally 10^{-2} – 10^{-1} per year
Category 5	Frequently 10^{-1} – 1 per year
Category 6	Very frequently > 1 per year

Table 3-2 Example of probability categories

3.4 Identification of protection levels

The effectiveness of the protection levels must be assessed similar to the categories in Tables 3-2 and 3-3. For this purpose, measures are assigned categories of increasing effectiveness (e.g. from category A = highly effective to category F = ineffective). The measures are assigned via operationalized definitions of the categories.

The risk management system must include measures which ensure

- reduction in the probability or frequency of occurrence, and
- reduction in the *consequences* of an event.

The approach selected for this purpose must be logical and outlined in the pertinent documentation.

As a matter of principle, risk management systems should always aim to reduce risks to an acceptable level and pursue the necessary planning and implementation of risk reduction measures.

Failure to achieve this goal must be documented. If the risk is accepted nevertheless, the reasons for this decision must be provided. Alternatively, further risk reduction measures must be taken (even if this ultimately results in the discontinuation of a product or product line).

3.5 Nanotechnology-specific risk matrix

Considering the low level of knowledge concerning nanotechnology-specific risks, a suitable risk matrix must be defined. Figure 3-1 shows an example of such a nanotechnology-specific risk matrix. As in Figure 2-1, the consequences, in this case the possible consequences, however, are shown on the x-axis. Compared to Figure 2-1, risk categories are aligned more vertically therefore placing more emphasis on consequences.

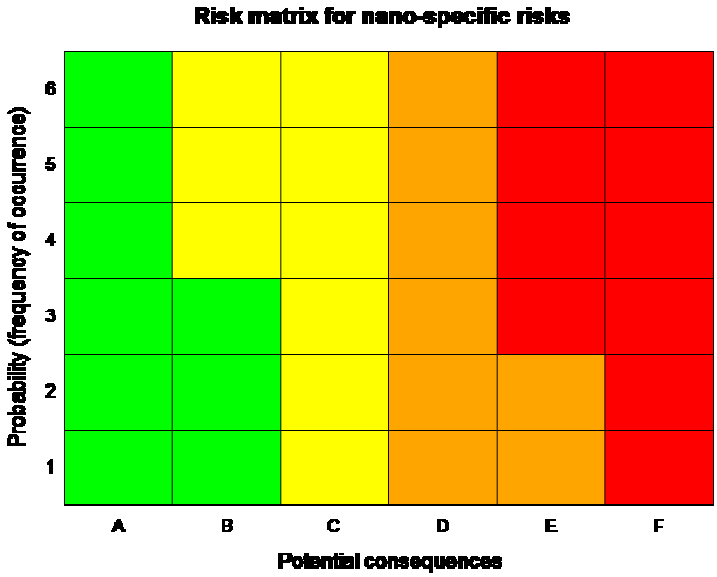

Figure 3-1 Risk matrix for nanotechnology-specific risks

The probability or frequency of occurrence is shown on the y-axis, e.g. in line with the categories of Table 3-2.

Product risks may also be mapped in the risk matrix: In this case, the company must identify the possible exposure scenarios, the expected normal use and reasonably foreseeable misuse. Here, the aspect of "probability" no longer plays a role as one must expect events to occur if products with clear safety defects are sold on the market. Therefore, product risks are always assigned to the highest category of probability (category "6" in Figure 3-1).

3.6 Risk control and periodic risk assessment

Changes in the operational processes for which the risk management system has been developed must be incorporated into the risk management system at regular intervals and the risks re-assessed.

These changes may vary to a great extent and may include necessary construction measures, introduction of a new supplier for individual products or recruitment of new employees. Apart from changes in business operations, there may also be changes in the company's environment which necessitate risk re-evaluation.

A risk management system must, therefore, include risk monitoring which identifies these changes at an early stage and thus enables the company to take the appropriate measures (Chapter 4).

Risk monitoring aims to identify changes in the environment which may influence the assessed risks at an early stage, re-assess these risks and take countermeasures, if necessary.

Risk assessment may not date back more than six months at the time of certification.

4 Risk Monitoring

Nanomaterials and products which contain nanomaterials form part of an interdisciplinary technology which is characterized by short cycles of scientific and technological innovation and knowledge and very much subject to the impact of regulatory measures and social trends.

To objectively assess the risks occurring in the various phases of the lifecycle of such products, a monitoring system is needed which reduces the increased level of decision uncertainty resulting from this.

4.1 Backing up the decisions

Corporate processes and products must be integrated into a suitable proactive monitoring system which provides reliable certainty for all decisions related to the production, marketing and sales of nanomaterials or products containing nanomaterials. Monitoring aims to identify and analyse current and future risks as extensively and early as possible. The objective is to enable the company, throughout all phases of the product lifecycle, to take effective and suitable measures at an early stage. Figure 4-1 shows the integration of continuous monitoring into the risk management process:

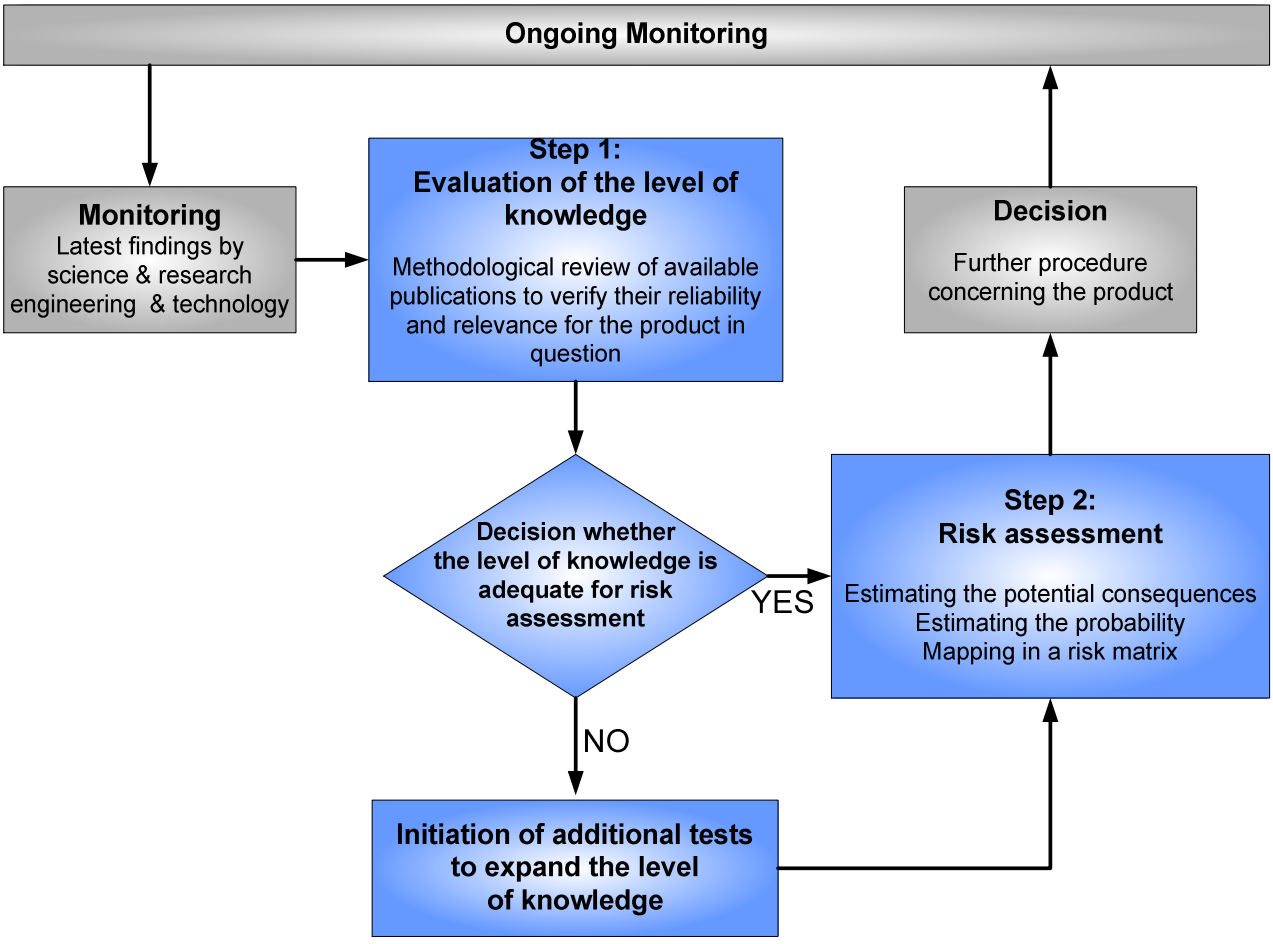

Figure 4-1: Integration of monitoring into the risk management process

4.2 Systematic data collection and analysis

Monitoring includes defined processes to support decision making:

- Systematic data collection and analysis
- Summarizing and linking of relevant information
- Deriving knowledge relevant for decision making

A monitoring system may cover very extensive aspects such as the monitoring of science and research, engineering and technology, society and legislature and market and competition. The CENARIOS® standard requires monitoring of the safety-relevant aspects (HSE risks):

- Science and research
  Human toxicology, ecotoxicology, occupational health and safety and environmental protection
- Engineering and technology
  Product and process safety, technical installations

As a matter of principle, these two areas should be monitored by means of an integrated approach to ensure the basis of decision making is as extensive and proactive as possible.

4.3 Feedback of experience

The monitoring system should take adequate account of operational experience and product experience and use them to summarize and link information. The feedback of experience must be used to derive knowledge relevant for decision making.

4.4 Transparency of the monitoring process

The monitoring process should be as transparent as possible. The selection and processing of the used sources of information and instruments must be documented, traceable and objectively justified. The collected data must be specifically processed and used with due technical care and in line with defined standards.

4.5 Continuity and topicality

The monitoring system ensures that progress in the collection of data and information is surveyed on an ongoing basis. Suitable measures must be taken to ensure that the monitoring system provides up-to-date findings and results. To keep the efforts involved in the operation of such a system at a reasonable level, recording all relevant changes in the above areas at three-month intervals will be sufficient. These changes must be documented, e.g. by identifying new publications with the date of purchase.

4.6 Data sources for monitoring

The system must always furnish traceable evidence which proves that the data sources used for monitoring are suitable to provide information about the state of the art in science and technology.

The type of these data sources is basically irrelevant provided evidence of their suitability has been furnished. In addition to commercial databases, we recommend the use of the findings and results of public research projects – e.g. the NanoCare project of the German Ministry of Education and Research (Bundesforschungsministerium, BMBF) as soon as this information is available.

5 Bibliography

ONR 49000 Risk Management for Organizations and Systems – Terms and basics – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49001 Risk management for organizations and systems – Risk Management – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49002-1 Risk management for organizations and systems – Part 1: Guidelines for embedding the risk management in the management system Practical use of ISO/DIS 31000; 2008-06-01

ONR 49002-2 Risk management for organizations and systems – Part 2: Guideline for methodologies in risk assessment – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49002-3 Risk management for organizations and systems – Part 3: Guidelines for emergency, crisis and business continuity management – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49003 Risk management for organizations and systems – Requirements for the qualifications of the Risk Manager – Practical use of ISO/DIS 31000; 2008-06-01

FERMA A Risk Management Standard, published by AIRMIC, ALARM, IRM: 2002

VDI Risikokommunikation für Unternehmen (ISBN 3-931384-33-0).

ISO/IEC Guide 51, 1999 Safety aspects – Guidelines for their inclusion in standards

ISO/IEC Guide 73, 2002 Risk Management – Vocabulary – Guidelines for use in standards

Environmental Defense/DuPont, 2007: Nano Risk Framework, June 2007

Directorate General for Environmental Protection at the Ministry of Housing: Physical Planning and Environment Premises of Risk Management, Dutch National Environmental Policy Plan, The Hague, 1988-1989

U.S. Environmental Protection Agency: A Summary of General Assessment Factors for Evaluating the Quality of Scientific and Technical Information, EPA 100/B-03/001, June 2003.

Industrie Service

Choose certainty.
Add value.

CENARIOS® Certification Standard
Part E

Requirements Related to Risk Treatment and Risk Communication

Date: 13 August 2008

Our references:
IS-ATC1-MUC

Document:
08-08-13 CENARIOS Certification Standard Part E.doc

This document consists of
9 pages
Page 1 of 9

Headquarters: Munich
Trade Register: Munich HRB 96 869

Supervisory Board:
Dr.-Ing. Axel Stepken (Chairman)
Board of Management:
Dr. Peter Langer (Spokesman)
Dipl.-Ing. (FH) Ferdinand Neuwieser

Telefon: +49 89 5791-0
Telefax: +49 89 5791-2888
www.tuev-sued.de

TÜV SÜD Industrie Service GmbH
Niederlassung München
Bereich Anlagentechnik
Westendstraße 199
80686 München
Deutschland

Industrie Service

Table of Contents

0 Preamble

This part E of the CENARIOS® certification standard[1] for risk management systems describes the requirements related to risk treatment and risk communication. The special requirements applicable to risk management systems according to the CENARIOS® standard result to some extent from the currently low level of knowledge in the risk assessment of nanomaterials.

0.1 Other applicable documents

These requirements to risk treatment and risk communication represent the fifth and last part of the CENARIOS® standard for risk management systems. Part A of the certification standard provides companies seeking to be certified with the preliminary information required in order to prepare for the certification process. Parts B to E of this standard contain more detailed information about the subjects addressed and aim to help companies to identify opportunities for improvement, if any.

Part A
Part A describes the general criteria and provides a summary of all subsequent parts of the standard. This part of the certification standard is based to some extent on *A Risk Management Standard* (FERMA).

Part B
Part B describes staff-related requirements, focusing in particular on the role of Risk Manager. This part is based on ON Rule *ONR 49003*.

Part C
Part C addresses all requirements associated with the organizational structure of companies, focusing in particular on the requirement that a company's organizational structure must facilitate the smooth implementation of a risk management system (*ONR 49002-1*).

Part D
Part D addresses the special requirements involved in the risk assessment of new technologies with small knowledge base. It also describes the requirements governing risk identification (monitoring).

Part E
Part E addresses the requirements related to risk treatment, including, firstly, pro-active risk communication and, secondly, an issue management strategy. Part E of the certification standard is based to some extent on the VDI brochure *Risikokommunikation für Unternehmen (Risk reporting in companies)* and on ON Rule *ONR 49002-3*.

[1] CENARIOS® is the legally protected name of the risk management system developed jointly by TÜV SÜD and Innovationsgesellschaft, St. Gallen, Switzerland.

1 General requirements for risk treatment

In spite of all efforts that have been taken, a company's image may suffer as a result of an incident, or the company be challenged directly with considerable or even existence-threatening financial risks. Incidents in other companies or involving other nanomaterials also may cause a change in public perception and thus turn into direct or indirect risks.

The risk management system thus must, firstly, verify that the company takes appropriate risk prevention measures and, secondly, provide risk treatment systems (e.g. issues and crisis management, documented risk communication procedure).

These general requirements for risk management systems to ensure risk treatment basically also apply to companies operating in the field of nanotechnology. As nanotechnology develops in an environment characterized by rapid changes, pro-active elements of risk treatment are needed, such as risk communication:

The CENARIOS® risk management system therefore must include

- risk communication, and
- issues or crisis management

schemes as integral elements of risk treatment. With respect to the risk communication scheme a pro-active approach should be chosen.

1.1 Approach to risk treament

Suitable measures must be developed to optimize the position of identified and analyzed risks. The task in hand is to ensure that all risks remain within defined and acceptable limits.

Suitable measures are also determined, to a certain degree, by the following requirements:

- ***legal requirements***, e.g. requirements governing the minimum capital base needed by banks or for adverse events associated with pharmaceutical products,
- ***official requirements***, e.g. requirements governing emission limits, or
- ***contractual partners,*** e.g. contractually agreed levels of quality

Basically, the following solutions are feasible:

- Improvement of information and communication processes: The more staff and executives are included and involved in these processes, the better the risk management process
- Preventive or mitigating measures: e.g. consistent implementation of certain organizational measures
- Internal measures of risk compensation: Risks are offset fully or partially in the company by adopting good business policy
- Third-party insurance: Against payment of an insurance premium, certain risks are transferred to the insurer
- Contractual transfer of risks to partners (e.g. suppliers) or the capital market
- Setting up risk management reserves: The company or a network of companies sets aside reserves to cover or eliminate damage caused by events.

For each individual risk, the company must select a suitable measure from the above solutions and, in this context, must also take corporate objectives into account.

2 Requirements related to risk communication / issues and crisis management

2.1 The modules of risk communication in brief

Issues and crisis management means addressing the issues that cause crises and treating crisis events. It covers tasks before, during and after a crisis. Communication is one of the key management tasks in this context. A crisis is defined as loss of control over business processes caused by public reactions to the company and may have significant impacts on the company's earnings and/or competitiveness.

The key tasks of issues and crisis management are summarized below:

- Identification of issues that may lead to crises: What appears to be happening?
- Forecast of possible "worst case" scenarios: What if...?
- Coordination and agreement of contingency plans: What preparations can be taken to improve crisis management?
- Acting in the case of a crisis: What must be done? What must be done and when?
- Regaining control: How can the company regain the initiative? How can the business segment be protected?
- Learning from crises: How good was the crisis managed? What can be improved?

This leads to the following general requirements for crisis management and risk communication:

- Preparing a crisis management plan,
- Setting up a crisis management team,
- Providing the logistical and technical resources required for crisis management,
- Running crisis exercises and crisis simulation to familiarize staff with the processes of crisis management.

2.2 Implementation-related requirements

Issues and crisis management and risk communication must basically cover the following stages:

2.2.1 Upstream crisis communication

The objective of upstream crisis management must be to prevent the crisis from occurring. Should a crisis occur nevertheless, upstream crisis management must have appropriately prepared the company. This involves the following tasks:

- (Human) resources planning
- Defining the roles and responsibilities in crisis management
- Identifying possible crises
- Evaluating and prioritizing potential crises
- Monitoring the development of potential crises
- Preparing preventive communication strategies by standardizing terminology
- Guidance on how to behave in important communication situations
- Communication training for staff

2.2.2 Communication during a crisis

If a crisis occurs in spite of all preventive measures, clear internal and external communication must be built up without delay and this must be appropriately prepared. This communication must aim to ensure a rapid alert system followed up by the right response.

For this purpose, the following tasks must be fulfilled:

- Crisis assessment by the level of severity
- Rapid alert of crisis management team
- Assessment of the situation: Analysis of the crisis with respect to symptoms and developments
- Limiting the impacts on health, supply security, reputation, workplaces and the company's productivity
- Defining the contents and target groups of communication and ensuring rapid information
- Monitoring and documenting the course of the crisis

2.2.3 Downstream crisis communication

Communication after a crisis must aim to prevent the crisis from persisting and/or being negatively associated with the name of the company in the long term. The company can achieve this goal by actively communicating the learning process resulting from the crisis to the outside world.

Key tasks of downstream crisis communication include:

- Attending to victims and their relatives after a crisis
- Internal analysis of the root causes and circumstances which led to the crisis and the communication processes
- Drawing the conclusions with respect to staff, organization, site, production, and product and implementing the necessary improvements.
- Information about improvements

3 Requirements for risk communication in the company

How risk communication is integrated into the company depends largely on the size of the company, its technical orientation and corporate goals.

Basically, there are four different models for the implementation strategy:

3.1.1 Model 1: Risk communication as an additional function of the OHS or Environmental Protection Manager

Risk communication may be delegated as an additional task to the individual in charge of HSE (health, safety and the environment) issues. This model may be considered by small and medium-sized companies with a low level of potential crises. In this model, the technical responsibility for HSE issues is extended by communication tasks which are carried out in close cooperation with Corporate Management.

3.1.2 Model 2: Staff function for risk communication

Medium- to large-sized companies with a limited range of subjects which may give rise to risk communication may opt for an organizational approach of medium complexity. This includes for example companies which manufacture and sell potentially hazardous products but whose production facilities do not involve any site-related risks. In many of these cases, a small staff unit consisting of some employees is established and assigned either to corporate management, corporate communications or a central research unit. This unit carries out possible cross-sectional tasks and coordination in relation to possible risk issues. This includes, for example:

- Monitoring of and active participation in the discussions held in technical committees (e.g. German Chemical Industry Association, German Electrical and Electronic Manufacturers' Association);
- Coordination and communication of information between technical departments and corporate communications;
- Monitoring of scientific discussions addressing risk issues;
- Technical consulting of corporate communications and corporate management.

3.1.3 Model 3: Risk communication integrated into Corporate Communications

Large-scale companies with pronounced strategic risks which are highly vulnerable to crises (e.g. multinationals in the chemical industry) must develop a very differentiated and at the same time deeply integrated organizational scheme because of the highly complex communication tasks. On the one hand, dealing with the various target groups and communicating promptly and expertly in different technical contexts requires a high level of differentiation and thus division of labour. On the other hand, a high level of integration is needed to ensure standardized measures across the various parts of the company. An organizational model catering to both requirements consists of corporate communications at company headquarters which has policy setting authority for decentral communication tasks. To be successful, communications between company headquarters and the business units must be closely networked in this model.

The required functional differentiation may be realized for example by establishing the following departments and functions within corporate communications:

- Principle communication issues
- Staff communication
- Press and public relations
- Corporate image and advertising
- Investor relations

Integrated corporate communications is generally assisted by other central support services, such as business and market analysis, market communications or publication services.

3.1.4 Model 4: Risk communication in a holding company

Some organizations have migrated from a corporate to a holding structure in order to be more flexible, gain market proximity and achieve higher economic transparency. The management of the holding company is not generally involved in operating responsibility and restricts itself to strategic portfolio planning, corporate development and the definition of framework conditions.

Operational responsibility, in contrast, rests with the independent corporate companies. The member companies organized in a holding structure are thus responsible for risk communication (to which model 3 would apply, in turn).

If a crisis grows and turns into a holding crisis, however, the holding company must assume responsibility for communications. In upstream crisis management, the holding company tries to establish a uniform (minimum) standard of risk communication across the entire group by introducing guidelines and support offers. Compliance with this uniform (minimum) standard must essentially be on a voluntary basis as the holding company's direct influence on the operating companies is limited.

4 Bibliography

ONR 49000 Risk Management for Organizations and Systems – Terms and basics – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49001 Risk management for organizations and systems – Risk Management – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49002-1 Risk management for organizations and systems – Part 1: Guidelines for embedding the risk management in the management system Practical use of ISO/DIS 31000; 2008-06-01

ONR 49002-2 Risk management for organizations and systems – Part 2: Guideline for methodologies in risk assessment – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49002-3 Risk management for organizations and systems – Part 3: Guidelines for emergency, crisis and business continuity management – Practical use of ISO/DIS 31000; 2008-06-01

ONR 49003 Risk management for organizations and systems – Requirements for the qualifications of the Risk Manager – Practical use of ISO/DIS 31000; 2008-06-01

FERMA A Risk Management Standard, published by AIRMIC, ALARM, IRM: 2002

VDI Risikokommunikation für Unternehmen (ISBN 3-931384-33-0).