LANUV
Kompetenz für ein lebenswertes Land

Landesamt für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfalen

North Rhine Westphalian State Agency for Nature, Environment and Consumer Protection - Department Plant and Process Safety -

Question List and corresponding Helps for supporting the evaluation of Safety Management Systems

in accordance with Annex III of the Major Accidents Ordinance 2017

State January 2018

Landesamt für Natur, Umwelt und Verbraucherschutz
Nordrhein-Westfalen (LANUV)
Leibnizstraße 10, 45659 Recklinghausen
Telefon 02361 305-0, Telefax 02361 305-3215
E-Mail: poststelle@lanuv.nrw.de
www.lanuv.nrw.de

Autor: Birgit Richter, Fachbereich 75 Umwelttechnik und Anlagensicherheit für Gefahrstofflagerung und -verladung
Translation: Andrea Gerstner, Fachbereich 75 Umwelttechnik und Anlagensicherheit für Gefahrstofflagerung und -verladung
Stefan Gebhard, Fachbereich 74 Umwelttechnik und Anlagensicherheit für Chemie und Mineralölraffination

Index:

SMS: Major-accident prevention policy and structure of the SMS 6

Question 1: How is the quality of the company's policy with regard to plant and process safety evaluated? 6

Question 2: How is the Major-accident prevention policy evaluated? 7

Question 3: How is the installation, implementing and maintaining of the safety management system (SMS) in the establishment evaluated? 11

Question 4: How is the documentation of the SMS in the establishment evaluated? 16

Question 5: How is the corporate Governance (CG) for the plant and process safety of establishments evaluated? 18

Question 6: How are the rules for the financial scope of plant and process safety evaluated? 22

Question 7: How is the review of the SMS documentation control evaluated? 22

Question 8: How is the arrangement for announcement of the company policy respectively the plant and process safety policy in the company evaluated? 23

Question 9: How is the involvement of the employees in configuration and implementation of policies and rules evaluated? 23

Question 10: How are the rules for checking the aims in the plant and process safety policy evaluated? 24

Question 11: How are the implementation of plant and process safety policy and the regulation extend of internal safety rules and regulations evaluated? 25

SMS: Organisation and personnel 26

Question 1: How are the rules concerning the organisation of the establishment evaluated? 26

Question 2: How is the assignment of responsibilities evaluated towards plant and process safety? 27

Question 3: How is the process of selection and assignment of competent personnel evaluated? 28

Question 4: How are the rules for the warranty of an adequate human resource evaluated? 29

Question 5: How is the process of familiarization, qualification/ of the employees evaluated? 30

Question 6: How is the process knowledge management evaluated? 33

Question 7: How are the rules for information flow in the establishment according to (safety-relevant) laws, regulations etc. evaluated? 36

Question 8: How are the rules the selection of external companies evaluated? 37
Question 9: How are the rules for handling external companies evaluated? 38
Question 10: How are measures taken to raise awareness of the employees for the need of continual improvement evaluated? ... 39
Question 11: How is the on-site presence of the plant and process safety officer evaluated? 39
Question 12: How are the rules for application of plant and process safety committees evaluated? 40

SMS: Identification and evaluation of major hazards 41
Question 1: How is the process of identification and assessment of major accidents being evaluated? 41
Question 2: How are the applied systematic methods being evaluated? 43
Question 3: How are the procedures for the determination and definition of the safety relevant parts of the establishments being evaluated? 44
Question 4: How are the procedures for the determination and fixing of the safety-related parts of the plants within the Establishment being evaluated? 45

SMS: Operational Control 47
Question 1: How are the arrangements for the entry control and the protection of the intervention of unauthorized persons in the operating area being evaluated? 47
Question 2: How is the IT security process in terms of plant and process safety being evaluated? 49
Question 3: How are the regulations for the control of operational procedures being evaluated? 54
Question 4: How are the regulations for the permit to work being evaluated? 55
Question 5: How are the regulations regarding the handling of instructions (work / operating instructions etc.) being evaluated? 56
Question 6: How are the regulations for (safety) trainings being evaluated? 58
Question 7: How are the elements of the operational communication and their documentation evaluated? 60
Question 8: How are the regulations for shift changes evaluated? 61
Question 9: How is the process „alarm management" evaluated? 62
Question 10: How is the Process for maintenance evaluated? 64

Question 11: How is the process for the guarantee of the proper implementation of (periodic) inspections evaluated? ... 70
Question 12: How are the regulations for the management and control of risks associates with ageing equipment evaluated? ... 72
Question 13: How are the regulations towards procurement of materials and equipment evaluated? ... 75

SMS: Management of Change (MoC) ... 76
Question 1: How is the management of change (MoC) being evaluated? ... 76
Question 2: How are the regulations for communication at the different stages of a Management of Change (MoC) evaluated? ... 79
Question 3: How is the scheme to ensure the completeness and updating of the operating documentation being evaluated? ... 80
Question 4: How are the regulations for a temporary shutdown of a plant in the establishment being evaluated?? ... 81
Question 5: How are the regulations for start-up a plant in the establishment being evaluated? ... 81

SMS: Planning for emergencies ... 82
Question 1: How are the regulations towards the process information to the public evaluated? ... 82
Question 2: How are the regulations towards the process planning for emergencies evaluated? ... 86
Question 3: How are the regulations towards the process preparation and review of documents for emergency planning evaluated? ... 89
Question 4: How are the regulations towards the process of emergency trainings and emergency plan testing evaluated? ... 92
Question 5: How are the regulations towards the establishment's authority to decide in emergency case evaluated? ... 95
Question 6: How are the regulations towards the notification requirement evaluated? ... 97
Question 7: How are the regulations towards the crises management group evaluated? ... 98
Question 8: How is the cooperation with the off-site emergency response and emergency rescue service evaluated? ... 101
Question 9: How are the regulations towards the equipment of the operational emergency response evaluated? ... 102
Question 10: How is the procedure towards the equipment of the establishment with required warning devices evaluated? ... 102

SMS: Monitoring Performance ... 103
Question 1: How is the process of safety management system review according to aims and regulations evaluated? ... 103

Question 2: How is the process of the audit system evaluated? 105
Question 3: How is the procedure to eliminate deficits that had appeared in the emergency trainings evaluated?..... 108
Question 4: How is the process “internal reporting system” or the regulations of registration and handling of incidents evaluated? 109
Question 5: How are the regulations for using safety performance indicators in the plant and process safety evaluated?..... 112

SMS: Audit and Review..... 116
Question 1: How is the systematic review and evaluation procedure of the major-accident prevention policy (MAPP) evaluated?..... 116
Question 2: How is the procedure of the systematic review and evaluation of the SMS (management review) evaluated? 118
Question 3: How is the safety culture of the establishment valued?..... 121
Question 4: How is the communication culture of the establishment valued? 125
Question 5: How is the error culture of the establishment valued?..... 127
Question 6: How is the resilience of the establishment valued?..... 128

Area **SMS: Major-accident prevention policy and structure of the SMS**

Area

SMS: Major-accident prevention policy and structure of the SMS

Question 1: How is the quality of the company's policy with regard to plant and process safety evaluated?

Help:

If an integrated management system exists, the quality of the company's policy (policy statement, vision, guidelines etc.) as well as the point of process safety according to the Major Accidents Ordinance has to be evaluated.
If the company exclusively has a safety management system, the following points apply for company's policy in the field of process safety.

The company's policy (policy statement, vision, guidelines etc.) has to include the following points:

- Naming the company's aims e. g. customer focus, competitiveness, health, safety and environmental protection, process safety including the order of priority.
- Written definition with binding character for all employees, e.g. signed of company's policy by the owner of a company.
- Naming of basic principles for reaching the aims.
- Regular reviews whether aims are reached.
- Preparation of necessary funds and human resources for reaching company's aims.
- Further education for the employees in process safety and environmental protection.
- Transfer of information (e.g. to competent authority, public).

The company's policy should be worded clearly and intelligible and has to be available for everyone.
If necessary, the employees should be involved in the creation of the company's policy.

In the hierarchy of the company's aims those who prevent major accidents and limit their consequences should take priority to other aims in case of an incident.

The given funds and human resources for process safety must be adequate particularly with regard to the hazard potential from the establishment/plant.
In the company's policy of the integrated management system the priority of the point plant safety has to be distinguishable. It has to be placed on a high level in different company's aims and has first priority in case of an incident. Other points from the company's policy such as basic principles or inspections also apply to the process safety.

Area **SMS: Major-accident prevention policy and structure of the SMS**

Question 2: How is the Major-accident prevention policy evaluated?

Help:

According to § 8 German Major Accidents Ordinance the operator of an establishment has to draw up a document in writing setting out the major-accident prevention policy (MAPP). The operator has guarantee the implementation of the MAPP by appropriate means and structures as well as a safety management system in accordance with the Annex III.

The MAPP has to be drawn before initial operation and meet the following requirements:

- It has to include:
  - The operator's overall aims and principles of action
  - The role and responsibility of management
  - The commitment towards continuously improving the control of major-accident hazards
  - Ensuring a high level of protection
- Periodically review and where necessary update the MAPP (at least every 5 Years) or in case of occasion (significant modifications, incident).

See KAS Leitfaden Nr. 19 "Leitfaden zum Konzept zur Verhinderung von Störfällen und zum Sicherheitsmanagementsystem" and KAS Leitfaden Nr. 29 "Besondere Anforderungen an Sicherheitstechnik und Sicherheitsorganisation zur Unterstützung von Anlagenpersonal in Notfallsituationen unter besonderer Berücksichtigung des Leitfadens KAS-20".

In the scope of an inspection the MAPP has to be seen and evaluated towards the requirements mentioned above. For this following hints:

Lower-tier establishments
According to KAS-Leitfaden Nr. 19 lower-tier establishments have to describe the fulfilment of obligations of the operator in accordance to German Major Accidents Ordinance in the MAPP together with other available documents.
Besides the company's policy/safety policy and the guidelines deriving therefrom, the MAPP should include:
(a) Which major-accident hazards can occur in the establishment?
(b) Which measures are provided to prevent major-accidents and limit their consequences?
(c) How is the orderly implementation of these measures ensured and
(d) How is the safety management system structured and implemented?

The written composition must be comprehensible in itself but may be not as detailed as a safety report with regard to the Major Accidents Ordinance.

Area **SMS: Major-accident prevention policy and structure of the SMS**

The MAPP should include:
1. Company's/ safety policy and guidelines
2. Structure of the safety management system (SMS)
3. Hazard potential of the establishment
4. Locality
5. Substances
6. Type of process or activity
7. Technical and organizational measures for preventing major-accidents or to limit their consequences and the implementation in the SMS

If there are other documents in the establishment (notification according to § 7 German Major Accidents Ordinance or safety assessment according to other sets of rules), the MAPP can refer to these documents. It is strongly recommended that the elaboration of the MAPP must be comprehensible how the operator of a lower-tier establishment guarantees that measures to prevent major-accidents and to limit their consequences are implemented.

For the documentation of the company's policy and SMS in the MAPP see the helps of the other questions of this area.

The operator of a lower-tier establishment should describe the substances or categories of the substances in the MAPP which cover the hazard potential of the establishment. Besides the amount and type of handling also the physical and technical safety as well as reaction technologically aspects of the substance data have to be documented. These details and impact data, limit and evaluation values are written down in the safety data sheet.
In view of the location there has to be a closer look at the neighbouring residential area and plants, objects requiring protection and special locations (hazard trough earthquake flooding etc.).
It should be clear which plants, plant components or activities are important in accordance to hazard or prevention of major accidents, e.g.:

- technical purpose and configuration of establishments/plants with unit operation (encased or free-standing, physical or chemical conversation, continuous or discontinuous, temporary storage of educts or products, handling of waste, exhaust fumes, manual filling possess),
- main characteristics of the reaction (e.g. pressure, exothermal reaction, special material properties). For the safety technical evaluation of exothermal reactions see "Technische Regel Anlagensicherheit: Erkennen und Beherrschen exothermer Reaktionen" (TRAS 410).

The operator has to describe in the MAPP the identified essential hazard potentials and hazards that are identified in the systematic appraisal of hazards and has to list the safety-related plant components.

Area **SMS: Major-accident prevention policy and structure of the SMS**

Related to this the measures should be specified which the operator has planned for reducing and controlling the hazard potential as well as limiting the consequences of major accidents.
Such measures can be technical or organizational and have to be integrated in the SMS. This can be realized in a table inclusive rules/ requirements of the establishment according to the Major Accidents Ordinance.

Upper-tier establishments
For upper-tier establishments there are detailed information in the safety report about the major-accident hazards, which measures are necessary to prevent such accidents and to limit their consequences.
A part of the safety report is a well-structured statement in writing of the SMS according Annex III Major Accidents Ordinance. It can include the MAPP.

An example is the sample chapter "Description of the SMS in the safety report“ („Darstellung des Sicherheitsmanagementsystems im Sicherheitsbericht“ /LANUV NRW, Mai 2007/).

Index:
1 General information
- 1.1 Structure of the company
- 1.2 Major-accident prevention policy
- 1.3 Safety culture of the company
- 1.4 Consideration of the human factor in the company

2 The Safety management system
- 2.1 Structure of the Safety management system
- 2.2 Organization and personnel
- 2.3 Identification and evaluation of major hazards
- 2.4 Operational control
- 2.5 Management of change
- 2.6 Planning for emergencies
- 2.7 Monitoring performance
- 2.8 Audit and review

3 Existing regulations and Documents
- 3.1 Organization chart
- 3.2 Index of the management manual
- 3.3 Register of all regulations in the establishment
- 3.4 Classification of the regulations/ instructions according to the requirements of the Major Accidents Ordinance

4 Annex

With regard to KAS-Leitfaden Nr. 29 it is possible to see the MAPP as a general process to reach, maintain and optimize the process safety. Such a process can be in-

spired by the systematic management concept of continuous PLAN-DO-CHECK-ACT Cycle (PDCA-Cycle).

The cycle is divided as followed:

- Safe Design (“PLAN“)
- Safe Production (“DO“)
- safe technology and safe organization (“CHECK)
- safe modification (also “Management of Change”, MoC) (“ACT”)

followed by safe Design (“PLAN) to begin a continuous optimization process.

According to Annex III the points of the SMS can be matched to the index named above as followed:

Safe design (“PLAN”): 2.3 and parts of 2.2
Safe production (“DO”): 2.4, 2.6 and parts of 2.2
Safe technology and safe organization (“CHECK): 2.7, 2.8 and parts of 2.4
Safe modification (also “Management of Change”, MoC) (“ACT”): 2.5

Area **SMS: Major-accident prevention policy and structure of the SMS**

Question 3: How is the installation, implementing and maintaining of the safety management system (SMS) in the establishment evaluated?

Help:

The safety management system according to the German Major Accidents Ordinance equates in the essential requirements to the general requirements of management systems.
That is why the general requirements of management systems are shown below followed by the specifications of the SMS. That means that has a process oriented approach, a hierarchic structure of the rules and documents as well as an evaluation cycles to guarantee a continuous improvement and modification process. The SMS has to base on the company's policy of process and plant safety regarding to the German Major Accidents Ordinance and has to be appropriate to the establishment's hazards, operations and complexity. Therefore the SMS is based on assessment of the risks. The SMS has to include the following points mentioned in the Annex III of the German Major Accidents Ordinance. These points have to be considered in the processes of the establishment:

a) Organization and personnel
b) Identification and evaluation of major hazards
c) Operational control
d) Management of change
e) Planning for emergencies
f) Monitoring performance
g) Audit and review

At an Inspection the following aspects can be considered:
It makes sense to see this question "How is the installation, implementing and maintaining of the safety management system (SMS) in the establishment evaluated?" in the context with the next question "How is the documentation of the SMS in the establishment evaluated?" because the structure of the regulations and documentation are an essential part of general requirement of a SMS. The structure of the regulations and their relationship should be illustratable. This generally illustrates the structure of the SMS, but it does not mean that there is a SMS in the establishment.

To evaluate if there is a SMS in the establishment and not only (single) organisational regulations, in addition the following two aspects have to be considered:

- Process and plant safety in the company's policy,
- Review cycles.

The following questions can be helpful:

Area SMS: Major-accident prevention policy and structure of the SMS

- How is the quality of the company's policy with regard to plant and process safety evaluated?
- How is the Major-accident prevention policy evaluated?

Area **SMS: Major-accident prevention policy and structure of the SMS**

Area SMS: Monitoring Performance

- How is the process of safety management system review according to aims and regulations evaluated?
- How is the process of the audit system evaluated?

Area SMS: Audit and Review

- How is the systematic review and evaluation procedure of the major-accident prevention policy (MAPP) evaluated?
- How is the procedure of the systematic review and evaluation of the SMS (management review) evaluated?

The adequate participation of the top management is an important requirement, that the SMS is practised (see question "How is the corporate Governance (CG) for the plant and process safety of establishments evaluated?", area Major-accident prevention policy and structure of the SMS).

If there are certificates in an establishment (e.g. DIN EN ISO 9001 Quality management systems – Requirements or DIN EN ISO 14001 Environmental management systems – Requirements with guidance for use), it can be expected that the general requirements of an management system (policy, structure of the regulations and documentation with process approach, evaluation/review cycles) are implemented. In this case it has to be checked if the requirements of the German Major Accidents Ordinance are implemented as well.

Whether the relevant processes demanded in the German Major Accidents Ordinance completely exist in the SMS of the establishment is asked in the following areas:

SMS: Organisation and personnel
SMS: Identification and evaluation of major hazards
SMS: Operational Control
SMS: Management of Change (MoC)
SMS: Planning for emergencies
SMS: Monitoring Performance (especially the processes internal reporting system and safety performance indicators)

The area "SMS: Identification and evaluation of major hazards" is the most important part for plant and process safety and is the basis to determine and implement appropriate measures to prevent and limit major accidents.

Establishments should have a reference matrix that covers the correlations between the regulations/instructions and the requirements of the German Major Accidents Ordinance. This matrix must be up to date. The operator of the establishment can use it to see if the SMS regulations include all points of the Annex III of the German Major Accidents Ordinance. For more information see KAS-Leitfaden Nr. 19, Annex 3 „Beispiel für die Darstellung der Zuordnung der Regelungen/Anweisungen des Betriebsbereiches zu den Anforderungen der Störfall-Verordnung". Annex 3 is an extract

Area **SMS: Major-accident prevention policy and structure of the SMS**

(chapter 3.4) of the puplication Landesamtes für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfalen: „Musterkapitel, Darstellung des Sicherheitsmanagementsystems im Sicherheitsbericht“.

Explanations to the general requirements to management systems:
A management system is a fixed and documentarily system of all organizational structures, processes, arrangements, measures and inspections for reaching given (company) aims.
A management system is marked by

1. A process oriented approach
2. A hierarchic structure of the rules and documents as well as
3. Evaluation cycles to guarantee a continuous improvement and modification process.

Explanations to the definition of process and for the understanding of the structured composition of a management system and of evaluation cycles:
A process is a system and a set of activities that interact to achieve a result.
The processes in a company have to be governed by it and are specific for the company. It is possible to relate the company’s processes to the type of a process such as leadership core or support processes. A process itself goes through all levels of a management system. It is specific for the company in which extend and depth or at which level aspects of a process are handled. (KAS-Leitfaden Nr. 8)
The content of the structure of a management system is deciding as well as the structure of the documentation.
The number and the nomination of the documentation levels in a management system are undetermined. It is specific and depends on the company.
For the structure the documentation levels have to be related. /KAS-Leitfaden Nr. 8/

This structure of an establishment SMS has to be visualized.

“The evaluation cycles allow a continuous improvement and modification process.
Changing conditions can be seen at an early stage in the regular revision and it can be reacted effective in time.
Furthermore the evaluation cycles enable the early identification of weak points and an effective learning from mistakes.” /Anlagensicherheit, B. Richter/

Evaluation cycles from a management system are known as PDCA-Cycle (Plan-Do-Check-Act-Cycle).

Explanations to the requirements of the Safety Management System accordint to the Major Accidents Ordinance:
The safety management system (SMS) according to the German Major Accidents Ordinance must correspond in the basic structure to the elements of a management system shown above. Besides other management systems the safety management system has the aim to implement the plant and process safety in accordance to the German Major Accidents Ordinance as a plant and process safety process. The intension is to prevent major accidents and limit the consequences as far as possible.

Area **SMS: Major-accident prevention policy and structure of the SMS**

These aims are part of the MAPP. A SMS is used for the implementation of the MAPP or the plant and process safety policy in all levels of the SMS.
If there is an integrated management system the plant and process safety policy have to be part of the company policy of the establishment.

The SMS has to be appropriate to the hazards, activities and complexity of the establishment and therefore needs a risk assessment.

There is an international basic norm for the management of risks in a company/ organization: ISO 31000 "Risk management – principles and guidelines". The term risk includes the “effects of insurance on aims, tasks and requirements” and involves chances as well as threats. The norm mentions as the basis of risk management 11 principles, i.e.

- Integration into the global organization of the company
- Top-down approach – risk management is the task of the top management
- Consideration of the PDCA-cycle and
- The risk management process

The risk management process includes the following steps:

- Contextualization (determination of general parameters, influencing factors, criteria that matter for the organization)
- Risk assessment composed of risk determination, risk analysis and risk evaluation
- Risk handling framed into communication/ consultation and monitoring/ checking

The aspects communication / consultation and monitoring / evaluation have to be considered at all steps.
The DIN EN 31010 „Risikomanagement – Verfahren zur Risikobeurteilung“ (risk management- procedure for risk evaluation) supports the ISO 31000 and guides to the selection and performance of systematic risk management procedures (about 30 procedures, e.g. Brainstorming, checklists, structural “what-if”-procedure, failure modes and effect analysis (FMEA), Multiple-criteria decision analysis (MCDA)).
Both norms 31000 as well as 31010 are not for certification.
This is different in the DIN EN ISO 9001 „Qualitätsmanagementsysteme – Anforderungen“ („Quality management system- requirements“); the version 2015 includes the new element “risk-based thinking” i.e. with the chapters 4.1.”comprehension of the organisation and their contents” as well as 6.1 “measures for the handling with risks and chances”.

The SMS has to include at least the following points according to the Annex III, Major Accidents Ordinance:

a) Organization and personnel
b) Identification and evaluation of major hazards
c) Operational control
d) Management of change
e) Planning for emergencies
f) Monitoring performance
g) Audit and review

Area **SMS: Major-accident prevention policy and structure of the SMS**

In practice point b) “Identification and evaluation of major hazards” is a process that doesn’t exist in companies which are not covered by the German Major Accidents Ordinance.
On the other hand there are manifold already existing processes in the company e.g. point a) “Organisation and personnel or c) “Operational control” with related process documentations e.g. employee selection and training or for maintenance and operating instructions for sequence of operations. In these documents of the establishments the specific elements of the German Major Accidents Ordinance have to be integrated, besides the obvious points from Annex III also the requirements from §§ 3 – 6 German Major Accidents Ordinance.

The elements of a SMS have to be fulfilled by every establishment. There is a difference according to documentation structure or the documentation volume of the SMS (see next question) which depends on size and complexity of the establishment (small or medium-sized company, big group).
If there is an integrated management system (IMS) it is important that the plant and process safety is implemented appropriately, that means that all elements of the SMS are included – the pure implementation requirements for health and safety and environment protection are insufficient in accordance to plant and process safety in the German Major Accidents Ordinance (example: Major accident in the BP refinery in Texas City march 2005, see KAS-Bericht Nr.7).

The right implementation of a (safety) management system results in transparency, clarity, and structure of rules in a company. A circumspect documentation keeps the knowledge of a company and updates it in addition.
Necessary condition is the right measure at the determination of rules and complexity of the documentation.
If there are too many rules without a responsible structure an over-organization is the consequence and contradictory rules or useless bureaucracies exist.
Chaotic conditions are the consequence of an insufficient amount of rules.
In principle there should be only rules which can be controlled by the management and can by example be observed by the superior. For a good working management system top Management has to demonstrate leadership and commitment with respect to the management system. An practiced management system is a control and leading system which can have effects on the behaviour of employees at every activity and every hierarchy or organization level of an establishment.

Area **SMS: Major-accident prevention policy and structure of the SMS**

Question 4: How is the documentation of the SMS in the establishment evaluated?

Help:

If a management system should be established in a company, at first an appraisal of all rules and documentations written down has to be organized. All sequences and processes have to be determined. This is important because the structure of the management system is geared to the processes- so-called process approach. All requirements and aims a company wants to implement are considered in the particular process.
That is why it has to be clear what the management system has to fulfil and implement, that means in accordance to the German Major Accidents Ordinance: plant and process safety but also e.g. quality, health and safety, environmental protection etc.
Furthermore the (documentation) structure of the management system has to be determined. If there are no parallel structures in a company but only one management system exists in a company which covers all requirements, it is called an integrated management system (IMS).
In the following the term “management system” is used. It can be an IMS which includes the SMS or a separate SMS.

There are rules for the documentation of the safety management system as well as for the regular revisions. The structure of the documentation is determined and there is a given form (written down, EDP-concerned, across the group, plant related, etc.)
For all named points there have to be determined responsibilities and expertise.

The structure of the documents has to be comprehensible: a hierarchy with a central theme.
That mirrors the permeability of a process through the different levels of the management system. It is specific for the company in which extend and depth or in which level aspects of a process are handled.

The structure of the documents can be visualized as a pyramid with e.g. the following levels:

- Company policy
- Management manuals
- Handling instruction
- Working instruction
- Further applicable documents, e.g. forms, user manuals

/KAS Leitfaden Nr.8/: “At the top of the document structure there has to be the company policy also named vision, policy statement, guidelines etc. the company policy describes the general aims and principles of the company and applies to the whole company sector.

Area **SMS: Major-accident prevention policy and structure of the SMS**

The following documentation levels are going to be more specific and detailed. At the same time the field of application is even limited e.g. a working instruction for a process of filling can be relevant and valid only for one department and not in the whole company. The number and the nomination of the documentation levels in a management system are undetermined. It is specific and varying for every company.
For the structure the documentation levels have to be related.
On the basis of the sample above it is shown that further applicable documents can be related to a working instruction or handling instruction. This instruction can be related to a chapter in the management system and this again can be related to a basic statement of the company policy. Backwards a relationship has to be established as well."

The level of handling instructions, also process description or management instruction etc., is an implementing rule for processes. That means that they include responsibilities and processes for implementation of an extensive sequence of operation e.g. shipment, production, maintenance etc.

In the content of handling instruction design it makes sense to differ the description of relevant documents for the process realization into specifications and demonstration documents. This differentiation results in clarity. Specifications are e.g. handling or working instructions or forms such as a checklist "Plant inspection BE1". If a form is filled out such as the checklist "Plant inspection BE1" it is a demonstration document. Other demonstration documents are credentials, verification certificates etc.

It depends on size and complexity of the company how extended and detailed the description and wording has to be.

In a small company the structure of the documentation can have only two levels additionally to the company and safety policy: Handling instruction and further applicable documents. If the small company does only have a SMS, it can be useful to implement the documentations of the SMS in the major-accident prevention policy (MAPP).
In this case the MAPP can be seen as the management manual.

With regard to the appropriate extend of rules it is relegated to the help to the question "How is the resilience of the establishment valued?" , area SMS: Audit and Review.

Area **SMS: Major-accident prevention policy and structure of the SMS**

Question 5: How is the corporate Governance (CG) for the plant and process safety of establishments evaluated?

Help:

Corporate governance in the plant and process safety can be understood as participation and engagement of the company's top management in regard to the company's process safety. As well as resulting of this, the implementation of process safety in the company's policy, concept or guideline etc. and corporate culture.

To evaluate the corporate governance there might be interfaces to i.e. the following questions:

Area SMS: Major-accident prevention policy and structure of the SMS

- How is the quality of the company's policy in regard to the plant and process safety evaluated?
- How are the rules for checking the aims in the plant and process safety policy evaluated?
- How are the rules for the financial scope of process safety evaluated?
- How are the implementation of plant and process safety policy and the regulation extend of internal safety rules and regulations evaluated?

Area SMS: Audit and review:

- How is the systematic review and evaluation procedure of the major-accident prevention policy (MAPP) evaluated?
- How is the procedure of the systematic review and evaluation of the SMS (management review) evaluated?
- How is the safety culture of the establishment valued?
- How is the resilience of the establishment valued?

In the scope of CG the top management has to realize the risks of the company's activities.
According to the OECD-Guidance "Corporate Governance for Process Safety, OECD Guidance for Senior Leaders in High Hazard Industries" (Juni 2012) the top management must weigh the major accident risks and the left general business risks and therefore the risk management with regard to process safety must have the same significance as other business processes, financial management, markets, investment decisions etc. inclusive.

Therefore the management of an establishment should be interviewed and give answers in the scope of an inspection.

Questions from the inspector to the top management (or members of the management who are responsible for process safety) could be:

Area **SMS: Major-accident prevention policy and structure of the SMS**

- Where do you identify the main risks for major accidents in the establishment?

-- (How do you evaluate the risks for major accidents in the context of other general business risks in the establishment?)

- Which decisions and measures did you make to prevent major accidents?
- How would you describe the safety culture in your establishment?

- especially the communication culture in the establishment?

- When was your last safety tour / audit / inspection or similar in the establishment and what did you notice?
- How would you react if a major accident occurs in your establishment?

For further questions see OECD-Guidance „Corporate Governance for process safety“ or according to german conditions the modified modul „Fragebogen Corporate Governance (Grundsätze der Unternehmensführung) zur Anlagen- und Prozesssicherheit (CG APS) of the Bezirksregierung Arnsberg NRW“.

In the case of an inspection hints whether process safety is considered according to CG can be found in documents such as business report/progress report/corporate governance report of the establishment.
There are risk fields and general measures described e.g. unter the headline company culture, finances, research and development, investments, personnel, sustainability, safety, environmental protection, IT-security. Details of process safety can be found e.g. in chapters sustainability or also safety or environmental protection. If indicators or characteristic numbers are part of the business report/progress report/corporate governance report this listing is also a positive hint (interface to the help of question “How are the regulations for using safety performance indicators in the process safety evaluated?”, area SMS: Monitoring Performance).

Further information:
The OECD-Leitfaden „Corporate Governance für die Anlagen- und Prozesssicherheit“ (2013 translated version of Corporate Governance for Process Safety, OECD Guidance for Senior Leaders in High Hazard Industries Juni 2012) mentions the essential elements of a corporate governance for plant and process safety. It is addressed to executive managers in the (petrochemical) industry and other industrial establishments with a high hazard potential that make decisions with an impact to the strategic focus and culture of a company, e.g. Chief Executive Officers, president, members of the management, board of management, business management, directors.
A short definition of corporate governance cannot be extracted from the OECD-Guidance.

Corporate Governance includes the regulation framework for leading and evaluate a company. Since 2002 the „Deutscher Corporate Governance Kodex“ exists in Germany which mentions the essential legal regulations and includes approved standards of a good and responsible corporate management. I. a. the board of management and the supervisory board should report about the corporate governance in an annual corporate governance report.

Area **SMS: Major-accident prevention policy and structure of the SMS**

According to wirtschaftslexikon.gabler.de there have to be regulations for CG from the view of economical requirements of good CG to the following four points:

a) Determination of over-all aims of the company that offers an acting maxim of the top management to manage interest conflicts between the reference groups in individual cases.
b) Structures, processes and persons of the management by which these aims can be reached.
c) Regular evaluations of the management activities for inventory and continuous improvement of the management modalities as well as
d) Proactive corporate communication to win and stabilize the confidence and thereby the finally necessary support of the reference groups by establishing transparency.

The „Deutsche Corporate Governance Kodex“ includes in chapter 4 “Vorstand“ (“management”) and there in the sub-chapter 4.1 “Aufgaben und Zuständigkeiten“ (“tasks and responsibilities”) i.e. the following:

4.1.3 The management has to arrange the observance of the legal regulations and internal company’s rules and works towards the respect of the allied companies (compliance).
4.1.4 The management has to arrange an appropriate risk management and risk controlling in the company.

There is an international basic norm for the management of risks in a company/organization: ISO 31000 "Risk management – principles and guidelines". The term risk includes the “effects of insurance on aims, tasks and requirements” and involves chances as well as threats.
The application of this standard should help companies to implement a risk management by a systematic identification and evaluation of the business risks and thus the company’s resources can be used effectively for the handling of risks.
An adequate risk management helps towards the achievement of company’s aims and thus is a part of “good” corporate governance. The process safety should be considered as a resource for the risk “major accident”.

Hints to corporate governance from wirtschaftslexikon.gabler.de:
Corporate Governance (CG) means the legal and factual regulation framework for company’s management and monitoring. In contrast to the internal legal structure of a company concerning primary the interior order, the keyword CG includes also questions to the implementation of a company into its environment.

Companies build locations of an input bundling of different protagonists or reference groups (e.g. shareholders, truster, employees, suppliers) for a work-sharing creation of value by a top management leadership.
Thereby the relationships of the reference groups are regulated in explicit and implicit contracts. The company’s governance set of problems can be traced back to the point that the concluded contacts are to a certain extent incomplete and the diverse reference groups (stakeholders) have different interests.

Area **SMS: Major-accident prevention policy and structure of the SMS**

Depending on their influences to the company's events the stakeholder can try to use the incompleteness of the contract in their favour and thereby on account of other reference groups.
Contracts are incomplete because they refer to transactions in the future or because not all (complex and unforeseeable) developments in the exchange relationship between the parties of contract can be regulated right and fair in all details. The mutual rights and duties of the contract parties can only be regulated (more or less) fragmentary in the contract.
All stakeholder groups could be exposed to risks from incomplete contracts, but generally they have the option to use this contract incompleteness for their benefit.
Incompleteness of the contract and differences in the positions of interests generally afford an opportunity and a motive to the stakeholders according to the considerations above to act opportunistic in self-interest.
At the same time they are subject to the risk and opportunism of the other stakeholders.
The company's events represent a complex network of exchange relationships between many actors with opportunism options and opportunism risks.
Regulations for CG generally have the task to limit the scope and motivation of the actors for opportunistic behaviour by suitable legal and factual arrangements.
They aim at positive market conditions for a productive value creation and a fair distribution of values by weighing the loss because of opportunistic behaviour (opportunism costs) and the expenditure of regulations (adjustment costs or governance costs).

Regulations of the CG can limit the scope and motivation of opportunistic behaviour but cannot solve all thinkable conflicts between the reference groups. A superordinate leading maxim is necessary to give the top management as the owner of the top authority to dispose an acting orientation in individual cases.
By the law in force the management is firmly bound to protect the company interests. Thereby the company interests are due to the appropriate consideration of the diverse single interests of all reference groups.

Regulations for CG can be divided into three regulating levels: At first legal regulations and sub-legal governance standards can be divided. Legal regulations are the result of a parliamentary legislative procedure and binding for all addressees of the concerned law. Sub-legal governance standards ("soft law") complete the significant legal regulations and should (more or less voluntary) become operative by the company's self-obligation. The group of sub-legal governance standards can be divided due to its application range into general regulations for a specific bigger group of the company (e.g. codes such as the Deutsche Corporate Governance Kodex) and company-individual guidelines.

Area **SMS: Major-accident prevention policy and structure of the SMS**

Question 6: How are the rules for the financial scope of plant and process safety evaluated?

Help:

There is a budget for the unit process safety that is sufficient calculated for routine investment as well as special expenses (e.g. special investment, rapidly available means).
Criteria for sufficient assessment are available as well as rules for the release of funds. Beside criteria such as financial yields the rules should include the criteria improvement of process safety.

Question 7: How is the review of the SMS documentation control evaluated?

Help:

There have to be rules for navigation of the (safety) management system documents in the establishment.
The following points have to be considered: design, modification, regular review of specifications and status quo (e.g. all 3 years), evaluation and approval, distribution, appropriation, discontinuation, archiving.
The responsibilities, expertise of the employees and authority for the points/duties above have to be clearly defined.
Big companies generally realize this at the level of handling instructions/process descriptions etc.
In small companies it may be e.g. a chapter in the management manual.
The regular review of rules for document navigation has to be ensured by e.g. an audit system.

Area **SMS: Major-accident prevention policy and structure of the SMS**

Question 8: How is the arrangement for announcement of the company policy respectively the plant and process safety policy in the company evaluated?

Help:

The employees know the company's policy and plant and process safety policy. This is guaranteed in different kinds of dissemination and also checked.
The employees have access to the current issue of the policy statement, e.g. by a bulletin on the notice board.
It must be visible, that it is the current issue of the policy statement.
New employees get a copy of the current issue of the policy statement and are shown where to find information.
There are rules how outside company employees are informed about the policy statement. There are determined responsibilities for different aspects of the announcement of the policy statement.

Question 9: How is the involvement of the employees in configuration and implementation of policies and rules evaluated?

Help:

This is an aspect of safety respectively the communication culture of the establishment (see area „Audit and review "). The company / plant and process safety policy and consequential rules are topics in e.g. operations meeting, appraisal interview or audits.
The consequences at default of policies/ following rules have to be fixed and have to be counteracted.
This is also possible across levels in the hierarchy. There is a suggestion scheme with inducement for occurred proposals (immaterial/ financial).

Area **SMS: Major-accident prevention policy and structure of the SMS**

Question 10: How are the rules for checking the aims in the plant and process safety policy evaluated?

Help:
The aims can be divided into three aim levels (aim pyramid):

- **Normative aims** (global aims, indicator aim):
  e.g. object of a company, policy, vision or guidelines of a company/ organization: general aims, which determine the fundamental principles of the company (corporate identity). In case of three levels the business objective is part of the normative aims. In case of 4 or 5 levels the business objective is listed separately.
  Planning interval: *long-term* e.g. company's policy/ guidelines e.g. 5-10 years, company's aims 3-5 years.

- **Strategic aims:**
  implementation of global aims into convertible aims for the next company/organization level: e.g. increase the competence of personnel in the company in the field of process safety -> perform a program to increase the notification culture in the establishment.
  Planning interval: *medium-term* (1-3 years)

- **Operative aims** (action aims): Implementation of strategic aims into sub-aims for functional units of the company that can be measured and are date related (fulfil SMART-criteria) e.g. trainings for notification of incidents.
  Planning interval: *short-term* (< 1 year)

The aims are easy to check if they are conforming to the SMART-criteria (relevant for control, measurable, ambitious, realistic, appointment related).

If this is not possible (yet) due to the existing circumstances indicators can be used (alternate parameter which correlates with the relevant parameter and reproduces the parameter/matter of fact approximately.). (See help to the Question "How are the regulations for using safety performance indicators in the plant and process safety evaluated?" in area "Monitoring Performance ").

There have to be rules for periodic inspections of the company's policy and the safety policy which are also valid for plant safety.

Generally this is part of the management review, see help to the question "How is the procedure of the systematic review and evaluation of the SMS (management review) evaluated?" in the area "Audit and review".

Important is the implementation of general aims of process safety trough sub-aims of all levels in the establishment such as production. Furthermore it is important that the

establishment equilibrates the aims so that safety is not going to be secondary because of too high stress in production.
KAS-Leitfaden Nr. 29: It is to prevent that in the description of the management system aims of safety are accentuated whereas in daily routine only economic aims are important. Also in the appraisal of achievement both aims have to be integrated that a balance of the aims is possible.

There are fixed dates for the inspections (e.g. one a year, at different occasions). The responsibilities are clearly, without interruption and with a definite decision-making authority. The administration of a business/management is involved in the inspection procedure.

Question 11: How are the implementation of plant and process safety policy and the regulation extend of internal safety rules and regulations evaluated?

Help:

For the Implementation there is a system (e.g. risk management, risk evaluation, structured setting of the SMS). All aspects of the company's policy (policy statement, vision, guidelines etc.) have to be implemented in regard to plant and process safety. The employees are involved.
There are determinations for the inclusion of policy statement modifications in the safety guidelines. The responsibilities for the points above are fixed.

At purchasing and assignment of externally processed order plant and process safety is considered as well. E.g.an order is placed to an external company which ensures that they comply with the policy statement/ safety guidelines even if they are not the cheapest.

The extend of rules should

- cover all points of the policy statement
- consider the area of plant and process safety
- be manageable for a single employee
- be comprehensible for the employee
- be implemented locally
- be up to date

The responsibility and expertise for all points above have to be clearly defined.

Towards an adequate extent of regulations see help to question "How is the resilience of the establishment valued?", area SMS: Audit and Review".

Area **SMS: Organisation and personnel**

Area

SMS: Organisation and personnel

Question 1: How are the rules concerning the organisation of the establishment evaluated?

Help:

The overall organization of an establishment has to arrange a framework for reaching the aims by making arrangements and by performing work-sharing tasks.
The result is an overall organization structure that is divided into operational and organizational structure.

The **organizational structure** of an establishment represents a hierarchy of organizational units (departments, occupations) within their responsibilities and communication relationship. Graphically it can be displayed as an organigram.
Important is that there is an adequate correlation between task, responsibilities, essential competences, authorities and rights.

The **operational structure** shows the arrangement of operational sequences and processes. This arrangement of operational procedures is settled in the existing overall organization structure.

The responsibilities are documented in writing, e.g. in an organization chart, in job descriptions and descriptions of functions. Tasks, functions, responsibilities and authority are clearly assigned to them on all levels down to the operating personnel.
Are there organigrams: Yes/no?
If yes-> which? Unambiguous assignment?

Authorized commissioners (e.g. immission control or hazardous incidents commissioner) or internal services (e.g. security guards, plant fire brigade) are involved in the overall organization and interfaces are defined.

A conflict of interests by the task assignment (e.g. hazardous incidents commissioner and facility manager) has to be prevented.
Authorities and time resources are distributed uniformly that the related responsibility can be administrated.

It has to be guaranteed that the staff members have the expertise needed for carrying out the assigned tasks.

There is a system or regular reviews to recognize and eliminate failures in the responsibility and competence correlation.

Area **SMS: Organisation and personnel**

Staff menbers can get information about assigned responsibilities of all employees of the establishment.

Question 2: How is the assignment of responsibilities evaluated towards plant and process safety?

Help:

The responsibilities for plant and process safety are appointed (including deputies) and documented in writing.
The task assignment is appropriately related to the responsible person and there are criteria to determine them.
If necessary there is a hierarchic transfer of responsibilities to other levels at last to the operator level.

The transfer of tasks is done in writing. The document contains information about

- the transferred duties
- authority
- name of the assignee

as well as the signatures of the employer and of the assignee.

Area **SMS: Organisation and personnel**

Question 3: How is the process of selection and assignment of competent personnel evaluated?

Help:

The process and assignment of suitable personnel (personnel planning) is documented in writing. The following aspects have to be considered

- Responsible persons for the selection of suitable personnel have to be defined (e.g. committee)
- The organization of this process due to the interfaces between personnel and operating department
- Criteria for selection are set, e.g. education, professional experience, social skills needed for the job, responsibility.
- For the occupation/responsibility there are job descriptions and functional descriptions
- The criteria professional requirements and also requirements for safety engineering health and safety measures and human factor ("Human factors" are related to factors of the environment, organisation and work as well as human and individual characteristics which have a safety and health relevant influence to the work behaviour (Health and Safety Executes (HSE),UK, 1999).

It is important to keep the rules for the employment of suitable personnel in safety issues or as responsible person according to the German Major Accidents Ordinance in mind.

The process "personnel planning" has to be documented in a procedure/process description / management instruction etc. The documentation has to include:

- Aims
- Application range
- Definitions
- Description of the process steps
- Determination of the process step and task contents
- Determination of task competences and responsibilities
- Consideration of process interfaces
- Determination of the process step documentation content

The points above count for medium-sized and big companies, which have a personnel division. Small companies with e.g. three managers (owner, operating engineer, technician) have to document their criteria e.g. in a chapter of the Management manual (½ - 1 page) according to the German Major Accidents Ordinance.
Regular reviews have to be done to evaluate the contents of the process personnel planning (i. a. criteria, process, responsibilities).This can be realized e.g. in audits.

Area **SMS: Organisation and personnel**

Question 4: How are the rules for the warranty of an adequate human resource evaluated?

Help:

Staff members are appointed in an adequate quantity and according to their abilities so that the given tasks can be executed without difficulties. If, due to the size of the establishment, only one person is in charge of the field plant and process safety that person should have the possibility to draw on staff members working in other areas who have been trained accordingly, or on outside companies. Criteria (e.g. recording the time a work procedure takes, staff size developed over the years, minimum staff size required) for determining the staff size have been laid down and are to be taken into consideration. Factors such as inappropriate operation, transfer times, sickness, vacation are taken into account for determining the required staff size. Rules are set that deal with the question of how to proceed when the minimum staff size is not present (assignment of other personnel to step in, taking installations or parts of them out of order).

Area **SMS: Organisation and personnel**

Question 5: How is the process of familiarization / qualification of the employees evaluated?

Help:
The process of familiarization and/or qualification/training in the establishment is documented in writing. The following points have to be included:

1. process and responsibilities for familiarization
2. process and responsibilities for training and qualification
3. Interfaces from personnel and operating department

If necessary the familiarization can be seen as a part of the Qualification.

The training or qualification of the employees should be done in a qualification process (KAS-Leitfaden Nr. 20). According to the PDCA-Cycle the following points should be part of it:

- **Determination of the qualification process**
  - At the beginning of the qualification process there are the qualification aims. The basis for this purpose is the determination of necessary competences for the job/function/task (demand analysis). Important is an exact task-related description of the target competences within verifiable criteria (target-determination)
- **The state analysis**
  - Registration of the existing competences on the basis of determined criteria
- **Target-performance analysis**
  - Identification of the differences between specified target competences and existing competences of the employees. There are no measures to be taken, if there are no shortfalls.
- **Implementation of a qualification plan**
  - Shortfalls have to be specified and evaluated if they can be equalized by qualification measures or if the qualification measures are suitable for it (e.g. on-the-job Training, workshops for knowledge transfer, simulations and practical exercises for the transfer of skills).
  - Usually there is a catalogue for learning target.
  - (The KAS-guideline No. 20 exemplifies catalogues for learning target in Annex II. These include “human error”, “capacity and capacity limitation” and “risk sensitiveness and risk assessment”.)
  - The entirety of measures for all concerned employees results in the qualification plan.
  - Appropriate workshops, institutions, coaches have to be identified before qualification measures can be implemented.
  - An interface to other processes of the establishment can be created (e.g. purchasing department).
  - In this case it is important that to guarantee the quality of the qualification measures.

Area **SMS: Organisation and personnel**

- **Implementation of qualification**
  Implementation of the selected qualification measures by means of the qualification plan.
- **Qualification results**
  The efficiency and success of qualification measures has to be verified.
  When the qualification procedure is completed the competences have to be evaluated (independent from coach and exercise) – a repetition of the state analysis of coached employees.
  The following target-performance analysis shows whether the asked target competences are given.
  Are asked target competences available (no difference in the target-performance analysis) the qualification target is reached.
  If not, the qualification measures have to be developed.
- **Qualification modification**
  Comparison of qualification measures and qualification requirements.
  The qualification measures have to be verified if they are suitable for reaching the qualification target. If not, reasons have to be identified and appropriate conclusions have to be drawn (e.g. other workshops). If the necessary competences cannot be reached by qualification measures there have to be work structuring or organizational measures for troubleshooting.
  The cycle should be regularly run through, also after special occasions e.g. after safety-relevant modifications, within the need of other competences.
  An occasion can also be an incident (e.g. almost accidents).

The process “qualification” has to be documented in a procedure/process description/ management instruction etc. The documentation has to include:

- Aims
- Application range
- Definitions
- Description of the process steps
- Determination of the process step and task contents
- Determination of task competences and responsibilities
- Consideration of process interfaces
- Determination of the process step documentation content

The points above count for medium-sized and big companies, which have a personnel division. Small companies with e.g. three managers (owner, operating engineer, technician) have to document their criteria e.g. in a chapter of the Management manual (½ - 1 page) according to the German Major Accidents Ordinance.
Regular reviews have to be done to evaluate the contents of the process Qualification (i. a. criteria, process, responsibilities).This can be realized e.g. in audits.

Area **SMS: Organisation and personnel**

Annotation 1: familiarization

Aspects in the familiarization of newcomers:

New staff members are at first informed about the (company and) safety policy and Major-accident prevention policy of the establishment. A contact person (tutor) is available for new staff members during a defined period of time for answering arising questions. The tutor is granted time to assume this task and is relieved from other tasks. He/she needs to have the skills required for this task. The skills are checked periodically, e.g. by evaluations by the new staff members. There is an internal plan for acquaint new entrants with their job which schedules a gradual introduction to the new tasks to be assumed. There is one person responsible for following closely the foregoing items. A documentation covers all that.

Aspects for familiarization of employees at the beginning of a new task in a company:

At a new task by reason of changes in the field of responsibility (new technical equipment or technology) there are familiarization and qualification plans of the qualification process above.

Annotation 2: Qualification

Aspects for rules of employee qualification:
Funds and time are provided, that the employees can attend workshops, seminars, in-house qualifications etc. Every employee has his/her own plan for training and education. There are company-internal criteria (e.g. 1-2 workshops a year and employee, functionally, interdisciplinary, social skills offers) for the qualification plan.
Funds and time are provided that safety matter employees can participate in external workshops (VDI, VDE, VDS, GVC etc.) in the field of plant and process safety.
All staff members have access to continued education. A survey is conducted in regular intervals among staff members to determine the specific demand in continued education. The survey results are used in working out the education schemes and training schedules. All efforts with regard to continued education are documented. After certain events, e.g. major changes, failures, accidents in installations of e establishment, additional (educational) arrangements and trainings are offered. Responsible for all named topics have to be appointed.

Area **SMS: Organisation and personnel**

Question 6: How is the process knowledge management evaluated?

Help:

Knowledge management is the aware, specific and regulating handling with knowledge by a company (establishment). Knowledge in and of the company should be made transparent, (more) useable and appraisable. Data and information are parts of knowledge. Knowledge is developed by the combination of information with existing knowledge and includes know how in combination with feelings and perception (e.g. identifying an operation state of a machine because of heard noises). Knowledge needs the ability to establish interfaces or deductions and to do evaluations. This is implemented in actions and so serves for reaching aims, managing tasks and situations. Knowledge is bounded to the particular person and is supported by organization and technique.

Knowledge: information + experience + interfaces / deductions and evaluation.

To evaluate the knowledge management process of a company / organization there exist different level of maturity models.

In the context of the German Major Accidents Ordinance there should be information in the SMS of an establishment to the knowledge management in accordance to “safety-related” knowledge.
The answers to the following questions can be used (selection):

Area SMS: Major accident prevention policy and structure of the SMS

- How is the involvement of the employees in configuration and implementation of policies and rules evaluated?
- How is the installation, implementing and maintaining of the safety management system (SMS) in the establishment evaluated?
- How is the documentation of the SMS in the establishment evaluated?
- How is the review of the SMS document control evaluated?
- How are the implementation of plant and process safety policy and the regulation extend of internal safety rules and regulations evaluated?

Area SMS: Organization and personnel:

- How is the process of familiarization, qualification/ training of the employees evaluated?
- How are the rules for information flow in the establishment according to (safety-relevant) laws, regulations etc. evaluated?

Area SMS: Operational Control

- How are the regulations regarding the handling of instructions (work / operating instructions etc.) being evaluated?
- How are the regulations for (safety) trainings being evaluated?
- How are the elements of the operational communication and their documentation evaluated?

Area SMS: Management of change

Area **SMS: Organisation and personnel**

- How are the regulations for communication at the different stages of a Management of Change (MoC)?
- How is the scheme to ensure the completeness and updating of the operating documentation being evaluated?

At a high level of maturity the process knowledge management is determined in writing for medium sized and big companies. The following aspects should be included.

1. Aims that should be reached by the knowledge management (strategic knowledge management)
2. Procedure and responsibilities of the knowledge management process (e.g. areas, involved persons, documentation, process context/interfaces to-wards information, knowledge and competence management)
3. Description of the process steps (identify, generate, develop, win, distribute, apply, keep and keep available knowledge; operative knowledge management)
4. Determination of task competences/responsibilities
5. Consideration of the interfaces of other processes (installation of a SMS- regulations and documentation, organization and personnel – qualification of the personnel, audit system, internal reporting system, systematic review and evaluation)
6. Determination of documentation contents in the process steps.

Small and medium sized companies it is referred to the publication “Fit für den Wissenswettbewerb -Wissensmanagement in KMU erfolgreich einführen“ of the Bundesministerium für Wirtschaft und Technologie.

Hints/definitions/models of the knowledge management:

- **The “TOM-Model”:**
  The three competences technique, organization and human are part of the knowledge management.
  Techniques: information and communication technologies;
  Organization: development and implementation of methods for wining, memorizing and transferring knowledge;
  Human: creating general conditions for a friendly knowledge and learning company’s policy.

- **The “knowledge staircase”:** symbols (+ syntax =), data (+ meaning =), information (+ networking =), knowledge (+ application relation =), ability (+ desire =), acting (+ right acting =), competence (+ uniqueness =), competitiveness.

Area **SMS: Organisation and personnel**

According to the "knowledge staircase" **levels of maturity** can be defined (see reference: North, 2002):

1. level of maturity: **"IT-solutions"**: symbols, data
2. level of maturity: **"Special single solutions"**: symbols, data, information
3. level of maturity: **"professional knowledge management"**: symbols, data, information, knowledge, ability
4. level of maturity: **"knowledge orientated corporate governance"**: symbols, data, information, knowledge, ability, acting, competence, uniqueness

There is a differentiation between **explicit** and **implicit knowledge**, **internal** and **external** knowledge as well as **individual** and **collective knowledge**.
Implicit knowledge: unconscious (experience) knowledge
individual knowledge: knowledge of each single person
collective knowledge: knowledge of the business/ organization

Aims of the knowledge management are e.g.:

- convert implicit into explicit and individual into collective knowledge
- make external knowledge available for the business/ organization (promptly)

➔ make knowledge more useful for the business/ organization

Area **SMS: Organisation and personnel**

Question 7: How are the rules for information flow in the establishment according to (safety-relevant) laws, regulations etc. evaluated?

Help:

There is a structure of the company rule book, e.g. the binding character. The permanent topicality of rules and instructions as well as operation regulations is guaranteed. That can be realized by the subscription of learned journal or CD ROMs from a reliable source. For the information flow it can be helpful to participate in relevant committees and/or workshops.
The information flow responsibilities in the company are regulated clearly as well as the information transfer of new plant and process safety awareness.

There are well-defined elements in the company (e.g. meetings, research groups, objective agreement interviews, operating tours) which guarantee the information flow in the company see help to question "How is the process knowledge management evaluated?"
The workers' council is integrated in the information flow.
These elements are part of a process for formal internal communication (see help to question „ How is the communication culture of the establishment valuated?" in area SMS: Audit and Review).

Area **SMS: Organisation and personnel**

Question 8: How are the rules for selection of external companies evaluated?

Help:

Rules for selection of external companies are often placed in other processes of the establishment, e.g. purchasing department or personnel planning etc.
When selecting an external company special attention need to be paid to all safety aspects. Criteria for this may include various levels of safety requirements depending on the work to be done (e.g. service / maintenance work on safety-relevant equipment, carrier activities, work on buildings etc.). The responsible persons are to be named and the adherence to the safety standards is to be monitored.

Criteria for the selection of external companies have to be defined

- adequate qualification (education, professional experience, social skills of the employees)
- verifications (certificates)
- experiences of previous assignments
- work equipment facilities
- adequate human resources

The aspects of plant and process safety have to be part of the selection procedure of external companies and the external company content design.

Area **SMS: Organisation and personnel**

Question 9: How are the rules for handling external companies evaluated?

Help:

The rules for handling external companies are often hidden in other processes such as training, emergency planning, approval of dangerous tasks etc. It is important that the handling of external companies is an adequate part of these processes.

The following aspects have to be considered:

- It must be clear which persons, inclusive external employees, are in the establishment at present. This can be realized by a detection system.
- KAS-Leitfaden Nr. 19:
  At the application of external companies and their subcontractors there has to be documented how the necessary qualification of external employees, on the basis of rules defined in the SMS, is guaranteed and how the external employees are involved in the training and instruction system of the company. The plant and process safety issues have to be respected adequately.
  In the SMS there are procedures which regulate the coordination between external and internal employees (e.g. approval process and navigation of notations), the area of responsibility as well as the monitoring of the activity.
  The operator of the establishment is responsible for the coordination of the application of external companies (cf. § 8 ArbSchG, BetrSichV, TRBS 1112). Furthermore, it has to be described how an appropriate control of safety specification at operational use is guaranteed.
  How external company employees can introduce suggestions and indications of safety matter to the employer.

Rules must exist for the instruction of external employees. It is not necessary e.g. to instruct a painter who renovates the exterior of a building at the same level as a person performing preventing maintenance of a plant. The instructions should be given to the external employees and only in exceptional cases solitary to the director of the external company. The responsible person of the external company guarantees the adherence of the regulations.
A review of the instruction quality should take place, whether all staff members of the external company were addressed and whether they understood the instructions. The responsible persons have to be named.

In every case the adherence of safety relevant measures must be monitored. This monitoring should follow a systematic plan because there are differences in the levels of potential hazards of tasks (e.g. paint job versus maintenance work). The responsible persons (especially the interfaces to external companies), procedures and documentation of the monitoring must be defined clearly.

Area **SMS: Organisation and personnel**

Question 10: How are measures taken to raise awareness of the employees for the need of continual improvement evaluated?

Help:

It is important to sensibilise the employees of an establishment for the need of continual improvement. That means to recognize, communicate and implement aspects of plant and process safety improvement.
That is also an expression of a good safety culture (see Area SMS: Audit and review).
The continual improvement involves also that changes are recognized and an action is implemented.
The establishment can indicate special measures to improve awareness, e.g. campaigns of special themes, employee attitude survey, etc.

A promotion of the sensibility for plant and process safety improvement occurs by the implementation of e.g.:

- Qualification measures, implementation of awareness from operated (emergency) exercises.
- Good internal communication
- Internal suggestion system
- Internal reporting system
- Audit system
- Management reviews

A good implementation of elements named above shows that the PDCA-cycle is continuous and regularly ran through.

Question 11: How is the on-site presence of the plant and process safety officer evaluated?

Help:

Those responsible for plant and process safety are given enough of their hours of work (e.g. about 50 %) for carrying out their safety tasks in the installations they have been assigned to. A schedule of the time that is to be appropriated to each task should be available. Those responsible for plant and process safety should make inspections not only when asked to. They are expected to be present on the scene when safety relevant maintenance work is carried out as well as when failures occur, repairs are made and at similar events.

Area **SMS: Organisation and personnel**

Question 12: How are the rules for arranged plant and process safety committees evaluated?

Help:

Is there a documented process for formal internal communication (see help to the question „How is the communication culture of the establishment valued?" in the area SMS: "Audit and Review") If so, the application of safety committees should be regulated there.
There are rules for calling a temporary overall safety committee. This can be realized e.g. in an operating guideline. The responsibilities for the committee are regulated clearly as well as the participation and course of the committee meetings. The responsible person could be e.g. the facility manager of the affected establishment, someone of the administrative department or the commissioner. The direction of the committee should also be responsible for the calling of members. Safety committees are built regularly and at least in case of:

- Accidents
- near accidents
- modification of the plant
- disruption in operation etc.

The rules for the application of safety committees also include the aspect "implementation of decisions made by the safety committee".
The management of the concerned installation should be responsible for carrying out the measures, in any case those responsible for carrying out the measures should be officially appointed. The measures which are carried out need to be checked for example by the engineer of the installation or by safety experts. In addition, random checks are to be performed by someone not involved in carrying out the measures (e.g. the safety division, installation or company unit manager, members of the safety committee).

Area

SMS: Identification and evaluation of major hazards

Question 1: How is the process of identification and assessment of major accidents being evaluated?

Help:

The process for the identification and assessment of the dangers of Major Accidents in the operating area is specified in writing, e.g. in procedural instructions. The following aspects must be taken into account:

- Aims of the process for the identification and assessment of the dangers of major Accidents.
- Order of events and responsibilities of the process for the identification and assessment of hazard potentials (Concerning e.g. involved areas/people, implementation time, methods, documentation, conclusions, consequences)
- Description of the process steps
- Definition of responsibilities for the task
- Consideration to the interfaces of other processes (Especially MoC, but also e.g. Monitoring of the operation (alarm management), audit system, internal reporting system)
- Definition of documentation content during the process steps

The considerations above apply to medium-sized and large companies.

Small companies must set down their procedures and criteria in accordance with the requirements of the German Major Accidents Ordinance. Due to the different organizational structure, this part can take place e.g. in a chapter of the management manual. Aspects which can be described here could be:

- Timing of hazard analyses

and their basis / Implementation / execution e.g.:

- Own execution by the owner by means of the checklist <name, date, source specification> for the equipment <listing>
  - Explanation of how it is ensured that it is a current checklist / hazard analysis method

and /or

- Assignment of the risk analysis to a service provider, in principle or upon fulfilment of certain criteria, e.g.
  - A danger potential of the kind <name>, Special subject matter or special part (for example, fire protection system, refrigeration system), Participation of hazardous/dangerous substances <names of Substances> or every xx years
  - Identify and name the criteria that the service provider must meet in order to ensure an adequate quality of the risk analysis carried out on behalf of the contractor

Area **SMS: Identification and evaluation of major hazards**

- Contents of the documentation
- Dealing with the results from the risk analysis
- Ensure that the necessary measures derived from the results of the hazard analyses are also implemented (e.g., tools: to-do list with status indications, completed form sheets)

For all establishments, checks are periodically carried out, whether the established process and the responsibilities for the process for the identification and assessment of the dangers of Major Accidents are appropriate, e.g. in the context of audits.

Hints to the points above, e. g. process instruction:
The person responsible for selecting the members of the panel is named. Criteria for selecting the panel members are set, for example with regard to their knowledge in:

- installation systems and components
- process design
- dangerous substances
- methods applied in the hazard analysis
- Cybersecurity
- elements serving safety relevant functions (e.g. process control system, fire and explosion protection systems)

The conditions are set which determine when hazard potentials are to be identified and assessed. Examples are:

- process design
- new projects
- modifications of the installation (which?)
- addition of externally engineered systems or components to the installation, e.g. a refrigerating plant
- operational malfunctions (which?), Major Accidents
- maintenance work
- extraordinary operating conditions (e.g. start-up operation, emergency procedure).

Those responsibility for the identification and assessment of hazard potentials at predetermined times are appointed.

There are fixed criteria when which methods are to use (see also the answer of the follow-up question).

It is specified how the measures derived from the identification and assessment of hazard potentials are circumvented. The responsibilities who decide on the implementation of the measures and at which time this is done are defined. The responsi-

bilities for the implementation of the measures and for the verification, whether the measures have been carried out correctly, are laid down.

The topics of the hazard analysis to be documented and the style of their presentation are selected according to fixed rules. These topics may include:

- persons participating in the identification and assessment of hazard potentials
- object of the hazard analysis
- results
- concluded measures
- implementation of the measures
- check whether the measures have been implemented.

The duration of retaining the documentation and the persons in charge of the documentation are determined.

Corresponding to their importance for the target group the results of analysis have to be published (e.g. the publication is available for the staff of the establishment, other companies, public authorities, the professional community or the public at large). Criteria for these cases have been established. It is decided who is responsible for the publication (content, scope, time, etc.) and who is responsible for the execution of the publication.

Question 2: How are the applied systematic methods being evaluated?

Help:

It is determined which systemic methods are used. For large and medium-sized companies this is stipulated in writings in the process for the identification and assessment of the dangers of major accidents, e.g. in procedural instructions.
Systematic methods may include:

- check list
- HAZOP procedure
- matrix methods, e.g. Zurich matrix method
- index methods, e.g. Dow index method.

Criteria are determined for

- the conditions under which a method may be used, for example
- depending on the process
- depending on the hazard potential, e.g. if a certain amount of a dangerous substance is exceeded
- the scope to be taken into considerations.

The analysis covers both the regular and the inappropriate operation of an installation. There are rules which ensure that the applied methods are pertinent and up-to-date.

Area **SMS: Identification and evaluation of major hazards**

Question 3: How are the procedures for the determination and definition of the safety relevant parts of the establishments being evaluated?

Help:

In accordance with the definition in the German Federal Immission Control Act, an establishment is the entire area under the supervision of an operator as soon as dangerous substances according to Annex I of the German Major Accidents Ordinance may be available in a corresponding quantity in one or more installations of the area including common or connected infrastructures and storage.

The operator must determine the safety-related parts of his establishment (SRB in German). These are the parts of an establishment, which can cause a malfunction (Major Accident), in particular also those parts in which dangerous substances according to Annex I of the German Major Accidents Ordinance can occur or occur. An important, but not exclusive, criterion is the quantity of a hazardous substance. In addition, the characteristics of the used hazardous substances and the conditions under which they are handled or stored play a decisive role.
In addition to the installations, the activities within an establishment must also be considered, in which the risk of a Major Accident may occur. These two systems ("plant") and operations ("activities") form the safety-related parts of an establishment (as defined in Annex II, Section III, No. 1 of the German Major Accidents Ordinance).

Activities in which the risk of a Major Accident may exist are, for example:

- in-house transport,
- provision,
- storage,
- loading and unloading,
- manufacture of substances by chemical transformation,
- handling of substances (grinding, mixing, transfer, packing, etc.)
- synthesis and analysis of substances, e.g. in laboratories,
- paint,
- operation of refrigeration (plants).

Safety-related parts of an establishment (SRB in German) usually contain one or more safety related system components (SRA in German).

Area **SMS: Identification and evaluation of major hazards**

Question 4: How are the procedures for the determination and fixing of the safety-related parts of the plants within the Establishment being evaluated?

Help:

System components are safety-related if a Major Accident cannot be ruled out in the event of their failure or absence. This means safety-related system components (SRA) are all devices, machines, systems, equipment parts and devices whose design, nature and operation depend in particular on the safety of the installation and the limitation of a Major Accident. The safety-related system components are a result of the risk analysis.

The procedure for determining the safety-related system components of an establishment must be documented and regularly checked.

This may be e.g. in a procedural instruction “Process for the determination and evaluation of the dangers of a Major Accident".

In practice, the safety-related system components are divided into two groups:

a) safety-related system components due to their substance content

These are plant parts in which a substance according to Annex I Major Accidents Ordinance may be present or may arise in safety-relevant quantities. The quantity which is safety-relevant depends on the substance properties (toxic, combustible, explosive, self-igniting, etc.) and on plant and ambient conditions (dammed / uninsulated explosion, laughter size, etc.).

b) **Safety-related system components due to their protective function**

These are components which are a measure for solving a protective task, e.g.

- Devices for ensuring a safety-relevant mass or energy flow (for example safety valves, cooling systems, stop systems, torches, emergency power generator)
- Installations for fire and explosion protection (for example, fire walls, fire extinguishing systems),
- PCT (process control technology (PLT in German) – protection
- Facilities for detection (e.g. Smoke detection)
- Facilities for the discharge, disposal or restraint (e.g. dump pans) of hazardous substances.

As a pragmatic approach for the classification of safety-related system components (SRA) due to their substance content standard values are used in a first approach. When a standard value is reached or exceeded, a safety-related system component part is present. A single case test must be carried out when a standard value is ex-

ceeded. The report “Richtwerte für sicherheitsrelevante Anlagenteile (SRA) und sicherheitsrelevante Teile eines Betriebsbereiches (SRB)” recommends standard values for SRA of 0.5% and for some substances or substance groups of 2% of the quantities set out in Annex I, column 4, of Major Accident Ordinance and which are listed in table 1.

Further information from the enforcement aid to the German Ordinance on Major Accidents of March 2004:
In order to solve a protective task, as a rule, at least two mutually independent protective measures are to be provided so that even in the case of a failure of one protective measure at least one effective protective as a redundancy is maintained (redundancy). Passive devices are preferable to active ones. Active device are preferable to organizational measures. For the classification of PCT (PLT in German) devices, the execution, the operation, and the testing of PCT protection & damage limitation devices, please refer to the VDI / VDE Directive 2180.

Area

SMS: Operational Control

Question 1: How are the arrangements for the entry control and the protection of the intervention of unauthorized persons in the operating area being evaluated?

Help:

According to § 3 of the German Major Accident Ordinance, the operator has to take the necessary precautions according to the type and extent of the possible dangers in order to prevent accidents by interfering with unauthorized persons.

Regarding the measures to prevent unauthorized intervention and the entry control, attention must be paid to the integration in the safety management system and, in particular, to the design of interfaces (for example, the processes of hazard analysis or training or dealing with external companies or planning for emergencies). The safety management system must specify that compliance with the regulations is monitored (e.g. from the operational management, the safety specialists, from the plant personnel). Deviations have to be investigated and appropriate consequences have to be taken. Responsibility for accountability and verification must be clearly defined.

After the “Vollzugshilfe zur Störfallverordnung“ (execution assistance to the German Major Accident Ordinance) from March 2004 an unauthorized person in the sense of § 3 of the German Major Accident Ordinance is any person who deliberately acts with the aim of directly or indirectly causing damage. It is irrelevant whether the employee is an employee of the operator, a person appointed by him or a third party. Recommendations for assessing the dangers of unauthorized intervention are included in SFK-GS-38.

Elements from the guideline SFK-GS-38:
Safety-relevant systems are to be secured by the operators, particularly the authorities responsible for internal security, to prevent unauthorized intervention. In order to achieve these objectives, the following measures may be taken:

- The perimeters of establishments – or if appropriate the common perimeter in the case of industrial estates – (site fence, gates etc.) must be secured by technical and organisational means to ensure that unauthorised persons cannot gain access without using force (e.g. damaging site fence, attacking security staff) or fraudulent misrepresentation (e.g. forging site IDs) and that ingress by force is detected within a reasonable time (e.g. by means of alarm systems, video monitoring, patrols etc.)
- Non-site personnel should be identifiable, e.g. by openly wearing distinguishable site ID badges. Visitors and staff of external companies must be monitored appropriately. It is indicated to the interfaces to the areas SMS: organization

Area **SMS: Operational Control**

and personnel (use and handling of external companies) as well as SMS: planning for emergency (Help on the question "How are the regulations towards the process planning for emergencies evaluated?").

- The installations themselves are to be protected such that unauthorised persons cannot cause a major accident without internal knowledge and/or technical aids.

Proof of sufficient precautions, in particular of the operator (of the upper class) against the intervention of unauthorized persons, should be carried out as part of a safety analysis.

A safety analysis is the identification and assessment of possible interventions of unauthorized persons and the possible dangers resulting from by using systematic methods. Their creation requires, in particular, knowledge about possible motivations and possibilities for action by unauthorized persons. In safety analysis, the identification and assessment of the specific hazards situation (hazard analysis) is combined with the results of the determination of the hazard points within the scope of the hazard analysis which is already required in the safety report according to German Major Accident Ordinance. Safety analysis can be a prerequisite for the derivation of safety targets and the necessary safety measures in the context of the creation of a backup concept. Documentations, regular review and updating, for major changes and for special occasions, are recommended.

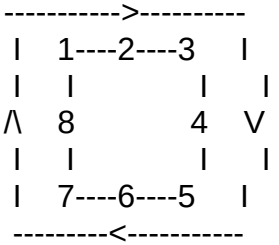
Area **SMS: Operational Control**

Question 2: How is the IT security process in terms of plant and process safety being evaluated?

Help:

Nowadays IT systems and / or industrial control systems (ICS), e.g. Process control systems (PCS) are used in establishments. In the past, ICS were “air gapped” (decoupled) from other IT systems and networks, and also from the Internet. This is increasingly changing, and IT security (information security, Cyber-Security, etc.) or parts thereof are also important for plant and process safety. The IT security measures in an operating area should not lead to essential services, functions or even emergency procedures being able to be not carried out. Since pure IT security targets focus mainly on the protection of the information, but not necessarily on the means of supply / plant, it can possibly lead to measures which are counterproductive for plant and process safety in the unfavourable case. On the other hand, IT security measures cannot be carried out at such a low level that the infrastructure is vulnerable by cyber-attacks or even unprotectedly connected to the Internet. It is therefore important to ensure compatibility with the various operational objectives in an establishment. The requirements for IT security are currently subject to a strong development and change process.

The German IT Security Act „Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes - BSI-Gesetz – BSIG vom 14. August 2009 “ (BSI Law - BSIG of 14 August 2009) requires operators of Critical Infrastructures to comply with legal requirements. Critical Infrastructures are of a certain size, e.g. refineries or tankers.
Within the scope of an inspection according to German Major Accident Ordinance, possible interfaces for plant and process safety must be observed, e.g. how the ICS of an installation/plant is taken into account in the course of the process model (here in accordance with VDI 2182 "Information security in industrial automation", page 1), how influences of IT security in alarm management are taken into account or whether sensors and actuators have remote access facilities (specific Device accesses, which usually use the Internet).
The procedure according to VDI 2182 includes the following steps:
1. Identify assets -> 2. Analyse threats -> 3. Identify relevant protection targets -> 4. Analyse and evaluate risks -> 5. Identify and evaluate risks -> 6. Select protective measures -> 7. Implement protective measures -> 8 -> 1. Identify assets ... ... in the sense of the continuous improvement process (PDCA cycle), step 1 is started after the 8th step and the cycle is repeated again (at regular intervals).



Area **SMS: Operational Control**

Definition "asset" in the sense of the guideline VDI 2182 Part 1: All material and immaterial values of automation devices, automation systems, machines or production facilities which may be threatened and which are protective (eg PLC, recipe, technical interface functions, firmware).
For medium-sized and large enterprises, the IT security process will usually be defined in writing, e.g. In procedural instructions, in which the following aspects are usually taken into account:

1. The objectives of the IT security process
2. Areas of application
3. Definition of terminology
4. Process and responsibilities of the IT security process, e.g. According to the VDI 2182 procedure (persons involved, implementation dates, areas, methods, documentation, conclusions, consequences)
5. Description of the process steps
6. Definition of responsibilities / responsibilities for tasks
7. Consideration of interfaces of other processes (e. g. Organisation and personnel (training, qualification, knowledge management), monitoring of the operation (including maintenance, alarm management), MoC, auditing system, internal reporting system, emergency management, management review)
8. Definition of documentation content during the process steps

Note on the procedure model above (process points No. 4 and 5):
IT components / IT based parts in plants have a very fast life cycle (for example for software components a time cycle of 1-2 years is clearly too long for certain steps within the procedure model).

Periodic reviews should be made as to whether the set out process and responsibilities for the IT security process are appropriate, e.g. In the context of audits.

In the case of inspections the following (critical) points of IT security can be inquired in connection with plant safety:

- Which regulations/guidelines of IT security are known in the company? Is there a documented procedure for the process IT-security e.g. in form of procedure/process descriptions?
- How is communication realized between the office IT and Process Control System? Are IT security specialists involved in hazard analysis for plant and process safety?
- How is the safety of the office IT with regard to the data transfer with the Process Control System seen? Which attack scenarios had been considered? Is cryptography (encryption) used? Where ? Are mobile devices used?
- In which form is Authentication, Authorization (Authority, management) and Accounting (Management of rights related to the IT), also known as Tripple A or simply AAA, implemented in the company/establishment/plant?
- How (secure) is the Login Process (password, other Provisions like a second authentication factor)?
- How is the interface designed between the management of change (MoC) and the IT-Security? Have changes in the context of EDP (e.g. new software or

updates) or IT devices been examined in its effects towards plant and process safety before realizing them? How are activation/ deactivation of features of new devices been realized?

- With regard to the plant that will be inspected: which networks exist? How secure are firewall, router and ports? Are virus scanners (AV Suits included) used and how secure are they (anti-virus protection)? Which data exchange exists?
- Is known which devices (also actors/sensors) in a plant have a remote-access specification (special device-specific port, usually using the internet or other common Network types)? How are they used (e.g. for maintenance purposes) and how are they protected (against unauthorized tampering)?
- Have the employees been sensitized for IT-safety? Are there/ have there been trainings/ campaigns?

Further Notes/Information:
IT security is about data security, i.e. the protection of data with regard to confidentiality, integrity and availability, as well as the authenticity, non-repudiation and accountability of data. Data protection, on the other hand, involves the protection of personal data against third-party misuse. Objectives and methods for data protection and data security can be the same, but this is not necessarily the case. However, IT security is usually a prerequisite for data protection, e.g. through access control.

The German Federal Office for Information Security (BSI) is a central office for questions on IT security and, in addition to the basic protection for IT security, also publishes information, technical guidelines and standards for IT security.
According to BSI, the following elements are important to the IT security process in an organization:
IT security is anchored in company's policy, which means there is a principle document (for example guideline for information security, security guideline, etc.) from the top management to the value, the basic goals and strategies of the IT security. The implementation of the IT security policy document is carried out by means of a security concept designed to protect the company's essential information and a process of IT security for the whole company. According to BSI important elements of the security concept are:

- **Structural analysis** is used to determine the assets to be protected by a company using:
    1. Listing of important information, business processes and applications,
    2. Network plan with IT systems, communication connections and interfaces,
    3. The existing IT systems (clients, servers, network coupling elements, etc.)
    4. The spatial conditions (real estate, buildings, rooms)

- **Security assessment / Protection requirement:** Which objects / assets can be infringed by the basic values of confidentiality, integrity and availability?

- Infringement of confidentiality: Can confidential information be unauthorized noted and / or passed on, and how can this be done (scenarios)?
- Violation of integrity: Can the correctness of the information and the functioning of the system no longer exist and how can this happen (scenarios)?
- Violation of Availability: Can authorized users be hampered by access to information and how can this be done (scenarios)?

- **Selection and adaptation of measures** using the IT basic protection building blocks - these are structured according to components, procedures and IT systems in the layer model:
  B1: Overlapping aspects,
  B2: Infrastructure,
  B3: IT systems,
  B4: Networks,
  B5: Applications.
  As well as hazard catalogues - these contain the essential hazards for information security, e.g. divided into:
  G1 Force majeure,
  G2 Organizational defects,
  G3 Human mistreatment,
  G4 Technical failure,
  G5 Intentional actions.
  And catalogue of measures - include measures to address the potential threats to information security, e.g. Divided into:
  M1 infrastructure,
  M2 Organization,
  M3 staff,
  M4 hardware and software,
  M5 communication,
  M6 emergency care.
  - Complementary safety analysis with an assessment of whether there is an additional need for analysis and, where necessary, covered by a risk analysis or possibly additional measures
  - re-examination of all selected measures and chosen/planed measures (= consolidated measures)

- **Implement measures**

The steps of the security concept above will be repeated at regular intervals to maintain IT security. This also verifies the implementation of measures and their effectiveness.

On the basis of the BSI IT-Grundschutz (BSI IT-Basic-Protection) it is possible to have an information security management system (IMIS) certified according to ISO 27001 "Information technology - IT security procedures - Information security management systems - requirements".

Area **SMS: Operational Control**

For fast, up-to-date security-related information on IT security, the BSI provides notification of the CERT-BUND (CERT-Confederation) on its Internet pages. The CERT-BUND enables companies to exchange security-related information and provides a warning and information service for IT security.

Hints to regulations (examples):

VDI 2182 „IT-security for industrial automation"
Part 1: General model
Part 2.1: Example of use of the general model for device manufacturer in factory automation Programmable logic controller (PLC)
Part 3.1 Example of use of the general model for manufacturers in process automation Process control system of an LDPE plant
Part 3.2 Example of use of the general model for integrators in process industry LPDE reactor
Part 3.3 Example of use of the general model for plant managers in process industry LDPE-plant

BSI (Bundesamt für Sicherheit in der Informationstechnik): IT basic security, information, technical regulations and standards for IT security (e.g. BSI-Standards – Methoden, Verfahren und Prozesse zur Informationssicherheit, IT-Grundschutz-Kompendium, IT-Grundschutz-Kataloge etc)
In connection with plant and process safety the ICS-Security-Kompendium has to be distinguished.

DIN ISO/IEC 27000 ff.: Information technology –Security techniques
27000: Information security management systems –Overview and vocabulary
27001: Information security management systems – Requirements
27002: Code of practice for information security controls
27003: Information security management systems — Guidance
27005: Information security risk management

DIN-IEC 62443 Industrial communication networks - Network and system security (formerly ISA-IEC 62443)

Area **SMS: Operational Control**

Question 3: How are the regulations for the control of operational procedures being evaluated?

Help:

There are two levels with regard to the control of operational procedures. On the one hand by the employees which are involved in an operational sequence, on the other hand by the control through supervisors or agents, e.g. within the framework of staff functions.

Regular rounds of the employees through the facility are used to record the operating status of plant components and their surroundings, often documented in checklists or logs. Deviations from normal operation should be recognized and reported by employees, including third parties.

Supervisor control is used to check the correct implementation of instructions by the employees as well as to provide information on the operating condition of the installation(s). This is done e.g. through tours, the viewing of shift books, discussions with employees, control of the processing of alarm messages, etc. These points may be part of a review of whether the content of work /operating instructions has been understood by employees and respected.

There are regulations on how to proceed if the content is not adhered to. In the case of infringements, it is appropriate to take clear and appropriate consequences for violations. However, this is to be practiced in an appropriate, graduated form which allows an open operating environment where cover-ups are not necessary (fault culture). It is important to consider the respective background of the violations and to take appropriate measures (e.g., in safety measures that affect the working process, to develop safety measures that do not interfere with the workflow).

Area **SMS: Operational Control**

Question 4: How are the regulations for the permit to work being evaluated?

Help:

For quite some time in factories permit-to-work procedures are common practice to deal with hazards that may arise in particular activities (e.g., flammable work, working in confined areas, opening of apparatus and conductors, work in potentially explosive atmospheres). The following points are, among other things, shown or regulated in the permit-to-work procedure:

- Responsibilities, responsibilities, powers for the respective points in the expiry of the approval procedure
- Activities (scope, location, duration)
- Hazards (e.g., personal injury, fire, release of hazardous substances)
- Protective measures (e.g., cleaning, freedom from hazardous substances, special tools, personal protective equipment (PPE), fire station)
- Control of the implementation (e.g., four-eyes principle)
- Completion and acceptance of the work

When regulating the permit-to-work procedure, attention must be paid to the integration in the safety management system, and in particular to the design for interfaces (e.g. to the processes of risk analysis or training or dealing with external companies, MoC). In the safety management system must be established that compliance with the permit-to-work regulations is monitored (e.g. from the operational management, the safety specialists or from the plant personnel). Deviations have to be investigated and appropriate consequences have to be taken. Responsibility for the competences and the review must be clearly defined. Corresponding regulations also exist for third-party companies.

Confusion between dangerous and "normal" work should not be possible. In this case the operator can access the process for risk analysis and the process for carrying out risk assessments according to the German Occupational Health and Safety Act.

Area **SMS: Operational Control**

Question 5: How are the regulations regarding the handling of instructions (work / operating instructions etc.) being evaluated?

Help:

Instructions are an important element in the SMS to ensure proper operation. When preparing instructions, aspects of occupational safety, environmental protection and plant and process safety must be taken into account. The operator must set down the procedures for creating, distributing and updating instructions in writing. For small businesses, this can be done in the management manual. For medium-sized and large companies, this should be defined and documented in form of a procedural description / process description / management instruction, etc. If necessary, the defined procedures and contents can also be found in other processes, for example, in the internal communication or control of documents. In any case, interfaces to other processes (for example, risk analysis, MoC, auditing system) must also be considered. Periodic verifications must be carried out, whether the established procedures and content are appropriate, e.g. in the context of audits.

Hints:
It is referred to the German Operational safety and hazardous substances ordinance and its technical rules e.g. TRGS 555 „Betriebsanweisung und Information der Beschäftigten“ ("Operating instructions and information of the employees") as well as „Handlungshilfe zur Erstellung von Arbeitsunterlagen für die Prozessführung" (“Aids for the preparation of work documents for process management”) from Lafrenz, Nickel and Nachreiner.

- It is necessary to define who is involved in the preparation of instructions; it may make sense to involve one of concerned employees.
- The instructions must be constructive, comprehensible and compliables.
- Relevant results from the process identification and assessment of Major Accidents are to be considered.
- The instructions have to be checked before they are put into effect.
- The topicality of the instructions must be guaranteed, this requires a clear responsibility. Criteria’s for updates should be defined (on a regular basis (e.g., semi-annual), on relevant changes to process, operational or work processes or legislation and rules, or after accidents (learned lessons)). Checks to see whether the updates are carried out, should have defined responsibilities and timelines - this can also be done in the context of an audit. Regulations for the transfer of these updates to the affected employees are important.
- The knowledge of the current instructions must be guaranteed. This can be determined, for example, by means of interviews or random sample surveys.
- The instructions not only regulate the normal operation, but also contain information on the behaviour in special situations (start-up and shut-down, maintenance operation, emergency situations, etc.) and indicate possible dangers and necessary precautions.

Area **SMS: Operational Control**

- Instructions must be accessible to all directly and indirectly affected employees and must be available in sufficient numbers. Instructions should be kept simple and comprehensible, for the sake of better understanding for foreign workers the existence in different languages also helps. Ideally instructions are available in all the languages employees in the company came from.

The instructions can be related to the workplace, activity and substance, and can, for example, describe responsibilities and regulate procedures and different operating modes, possible disturbances and the safety-related handling and measures in an emergency.

The instructions may include the following:

- scope: work area / activity
- hazard designation, hazards to man and environment (H-Phrases)
- protective measures
- rules of conduct
- hygienic measures (P-phrases)
- behaviour in the event of a disruption / dangers
- first aid measures
- proper disposal (in case of accident, leakage, etc.)
- if necessary also maintenance
- if necessary consequences in case of disregard.

Area **SMS: Operational Control**

Question 6: How are the regulations for (safety) trainings being evaluated?

Help:
By instructions / schooling employees' knowledge of the instructions (work / operating instructions) is regularly updated and rehearsed. The operator must specify (in writing) the procedure / instructions for carrying out the training. This can be done, for example, in the process of training and / or qualification / advanced training (see area: “SMS: Organization and personnel”, help to question "How is the process of familiarization, qualification/ training of the employees evaluated?"). Interfaces to other processes must be considered. Periodic verifications must be carried out, whether the established procedures and content are appropriate, e.g. in the context of audits. In this context Reference is made to the documentation requirements under the German Occupational Health and Safety Act and the technical rule TRGS 555 „Betriebsanweisung und Information der Beschäftigten“ ("Operating instructions and information for the employees").
Hints:
There are regulations for trainings, which take into account the following points:

- Responsibilities (who for what)
- Point in time / intervals of instructions (see 1)
- Criteria for the content (see 2)
- Which group of persons is affected
- Ensuring the participation of all concerned employees (for example: shifts, absence due to sickness or leave, employees of third-party companies)
- Review of Success of the learning (see 3)
- Documentation of Instructions (scope of documentation, retention period, responsibilities)

The contents of the rules on instructions and training are regularly reviewed, e.g. in the context of audits.

(1) Points at time / intervals of instructions, e.g.:

- Regularly
- Before
  - Undertaking new activities
  - Commissioning new / modified installations / equipment / work equipment
  - Changes of the process, operations and work processes
  - Relevantly amended instructions
  - Use of new substances / resources
  - Large-scale deposits / closures
- After
  - Accidents, incidents (fire, explosion, releases), Major Accident
  - New insights, e.g. By near-events

(2) Criteria for the content:
Instructions should address the dangers, their causes and the corresponding measures. The contents of instructions are also part of the documentation. Devia-

tions from normal operation are to be recognized and reported by employees, including third-party companies. In addition to instructions, training measures may also be required to support the appropriation of necessary competences.

(3) Review of success of the learning:
When it comes to training, small groups have more learning success than large groups. The learning outcome is checked, e.g. by staging a hypothetical incident, which can then be "edited" by a small group. However, there are also inquiries, written or oral tests.

Area **SMS: Operational Control**

Question 7: How are the elements of the operational communication and their documentation evaluated?

Help:
An important element for a safe operation process is the communication between the employees. Adjuvant is a cooperative behaviour of the employees among each other, in all hierarchic levels and between the hierarchic levels.

Important is a cooperation that enables an open and clear behaviour with mistakes in all hierarchic levels and all employees. The employees should get encouraged to notify occurred incidents, supposed hazards, near-accidents etc. and realise mistakes as a chance for improvement, learning effect and further development. But it also must be clear that vandalism effects appropriate consequences.

The leadership is efficient if the leadership behaviour, leadership expectations and task requirement fit to each other; this means that relationship maintenance, social distance, decision autonomy, planning commitments and communication style pass off as expected. For a good operational communication the span of control is also important. That means the number of subordinated employees of a manager has to be defined appropriately by the organization and is influenced by e.g. the following factors: task complexity, task interdependence, task homogeneity, technology, communication system, manager qualification, employee qualification, complexity and hierarchy structure of the company.

The communication between the employees is divided into a formal and an informal part. Both are important for the company performance.
The formal communication should guarantee an unobstructed internal communication flow, mostly organized permanently and not individually and essentially documented. Media of formal internal communication may be e.g. newsletters (if necessary standardized distribution lists), events (e.g. employees meeting), employee journal, management newsletter, appraisal interview, noticeboard etc.
Completed or replaced by electronic communication media such as E-Mail, Intranet, forums, newsletters etc. Also documents of the management system are in parts elements of the formal communication. Besides the general information flow, the focus at the review in accordance to the German Major Accidents Ordinance can be plant and process safety aspects.

In the following there is an exemplary list of communication elements in establishments:

- Information transfer in the line organization (meetings, protocols)
- Documentation at shift change (handover protocols, logbooks etc.)
- Notification of incidents/major accidents/ deviations from normal operation/ unsafe conditions
- Operating/work instruction
- Instructions (e.g. contents, in the framework of expectable changes)

Area **SMS: Operational Control**

- Operational suggestion scheme (filing, analysis and implementation of suggestion for improvement)
- Committees (agenda, protocols)

Regular reviews of the information flow and the procedure of the formal communication are useful. This can be done in the framework of audit systems.

Question 8: How are the regulations for shift changes evaluated?

Help:
The change of shift is of major concern to the safe operation of an installation. If, for instance, important information is not passed on to the next shift or if the installation is not supervised during several minutes of shift change, far reaching consequences may follow. Reliable flow of information may be realized by transfer protocols into which important data and changes concerning installation and process are entered. A brief dialogue between the operating staff of both shifts is also advantageous and should be required to secure safe operations as well as the transfer protocol.

Area **SMS: Operational Control**

Question 9: How is the process „alarm management" evaluated?

Help:
The alarm management is a systematic management of alarms in a process control system. It ensures reliability, productivity and safety of production-related facilities. A process "alarm management" should guarantee that the alarm system is correctly implemented, introduced, operated, maintenance and monitored.

Establishments which have no control room and where only singular alarms e.g. in the scope of gas or fire detection systems exist (e.g. hazardous substances depots, biogas plants) are exempt of the following statements of the process "alarm management".

The process "alarm management" should be determined and documented in writing in the form of procedure/ process descriptions or management instruction etc. The following points have to be included:

- Aims, that should be implemented and reached with the process "alarm management" (e.g. high functionality, effectiveness of the alarm system, optimal plant control),
- Application range (e.g. organizational units of the establishment, plants),
- Definitions (especially the terms alarm/ messages, safety related alarms)
- Description of the process steps and procedure of the alarm management
- Determination of the process step and task contents
- Determination of task competences and responsibilities
- Consideration of process interfaces (e.g. hazard analysis, MoC, internal reporting system, emergency planning, audit system),
- Determination of the process step documentation contents

Within the process "alarm management" the plant and control room personnel has to be involved adequately but also in the scope of creating the process instruction "alarm management".

The following statements are from the VDI/VDE 3699 sheet 5 "Process control using display screens-Alarms/messages" (September 2014) (in dependence on EEMUA No 191 and NAMUR NE 102):

An alarm is a message that demands an immediate reaction of the operator to prevent

- hazardous situations (early warning system to prevent emergency shutdowns) and/or
- economic damages (production quality and/or quantity).

The reaction in case of an alarm may e.g. be:

- operator interventions,
- increased attention (at the process monitoring),
- arrange further investigations.

Area **SMS: Operational Control**

An alarm has to possess the following characteristics:
relevant – clearly – modern – prioritized - understandable –diagnostic – indicative – focusing
(Indicative: An alarm helps to find the necessary behaviour. Focusing: An alarm leads to the important aspects.)

The following points have to be considered in the process steps:

- ergonomics
- determination of criteria that have to be fulfilled by the alarm system e.g. types of alarms (max. one alarm/10 min at normal operation; max. ten alarms/10 min in case of trouble)
- alarm configuration
- safety related alarms include the alarms PCS protective devises in terms of VDI/VDE 2180
- participation of the control room personnel at the single process steps, implementation of feedback
- special features such as staring and shut down procedures
- analysis of history, comparison of current state with the criteria
- assurance of the technical regulations up-to-dateness taken as a basis

For all establishments regular reviews have to be done if the determined procedures and responsibilities are appropriate for the process alarm management e.g. in the scope of audits.

For a deeper processing of the alarm management see the list of questions “Alarmmanagement“ of the LANUV NRW state April 2015. This list of questions and further information see LANUV Arbeitsblatt 27 "Leitfaden Alarmmanagement".

Area **SMS: Operational Control**

Question 10: How is the process for maintenance evaluated?

Help:
Maintenance
The definition in regard to TRBS 1112: combination of all technical and administrative measures as well as measures of the management during a lifecycle of work equipment (technical unit of a plant) for conserving the operational conditions or restoring them so that the required function can be performed.
The terms service, inspection and repair are parts of the generic term maintenance.
The definition according to BetrSichV: maintenance is the measures in total for conservation for conserving the operational conditions or restoring them. Maintenance includes inspection, service and repair in particular.

With regard to the terminology in connection with the maintenance see also DIN EN 13306 “Maintenance – maintenance terminology” as well as DIN 31051 “Fundamentals of maintenance”.

Maintenance also include improvements that increase the reliability, maintainability or safety of a technical unit, e.g. by eliminating weak points. A modification of a technical unit is not part of the maintenance if it should perform a modified function e.g. a higher performance etc.

A special area of the maintenance is the (periodic) inspection. If necessary there are special regulations for the areas maintenance and inspection (see help to question “How is the process for the guarantee of the proper implementation of (periodic) inspections evaluated?”).

At the (periodic) inspection the safety and performance of a technical unit gets evaluated by determined inspection methods, without further intended measures such as e.g. reparation.

In establishments the maintenance for the conservation of the ability to work is regulated long ago. i.a. also because of statutory provisions e.g. German BetrSichV and the associated technical guideline for general plant and process safety, especially TRBS 1112 maintenance (Instandhaltung). In the German Major Accidents Ordinance service and repair are mentioned explicitly (§ 6 Ergänzende Anforderungen und § 12 Sonstige Pflichten).

Mind the integration of regulations for maintenance in the safety management system and there especially the design of interfaces, e.g. to the processes hazard analysis, acquisition, qualification, handling with external companies, approval of hazard work, alarm management, emergency planning, audit system.
The involved appointments and their authorities as well as the responsible persons have to be determined clearly. Interfaces must be attended, especially if external companies are involved.
The regulations of maintenance have to be documented by the operator in writing. This includes also the identification and documentation of plant components of the

establishment that underlie the maintenance associated with a strategy and methodic for monitoring and inspection of the plant component condition.

For small companies the description of the procedure maintenance and responsibilities could be e.g. a part of the management handbook.

For medium sized and big companies this can be realized on the level of procedure/ process descriptions or management instruction etc. and has to be determined and documented in writing. The following points have to be included:

- Aims
- Application range
- Definitions
- Description of the process steps and procedure of maintenance (especially cooperation / interfaces of the different participants, e.g. department, maintenance, external companies)
- Determination of the process step and task contents
- Determination of task competences and responsibilities
- Consideration of process interfaces (e.g. acquisition, hazard analysis, MoC, audit system)
- Determination of the process step documentation contents

Regular reviews have to be done to evaluate the procedures and contents of the process maintenance (i. a. process, responsibilities, contents, interfaces).This can be realized e.g. in audits.

In the framework of the process “maintenance” there should be special attention on installation and shutdown procedures.

Hints from the TRBS 1112:
The TRBS 1112 describes the risk assessment procedure of maintenance work. It mentions exemplary measures that have to be considered at the performance of maintenance work with the results of hazard analysis. They have to be used for:

- Planning and performance of maintenance work
- Troubleshooting
- Testing after maintenance.

Before maintenance measures the following steps have to be done:

- Determine type, extent and procedure of the maintenance measures,
- Identify and evaluate hazards and determine necessary measures,
- Determine safety and qualification requirements of maintenance personnel before the allocation of external companies

If internal maintenance personnel are commissioned to perform tasks in the company, the employer has to instruct the employees about relevant hazards.

Area **SMS: Operational Control**

If there are different employers there have to be instructions between the employees of the involved employers in the scope of the coordination obligation regarding to § 8 ArbSchG. The instruction has to include information about local conditions, ongoing tasks in the company as well as corresponding hazards.

If there are acting employees in the environment of the maintenance work they have to be informed about the time, place and context of the maintenance work as well as possible limitations, hazards and the necessary consideration.

The performance of the work is only allowed if the determined measures are implemented. The determined measures have to be checked towards their effectivity. The following in particular:

- Preparation of the necessary work equipment and utilities
- Existence of the organizational requirements and complying them
- Determine the responsibilities
- Coordination in type and extent of risk prevention work and measures between the participants
- By site inspection of the operator's position is determined that the environment terms and conditions correlate with the presupposition
- Instruction of the employees

If divergent hazards are realized at the maintenance work of the risk assessment, works have to be stopped immediately but safely and the maintenance performing employer has to be informed. These have to determine the necessary additional measures, to instruct the personnel and to adjust the risk assessment.

During the performance of maintenance work the corresponding employer, which ordered these work, has to control the implementation and effectivity of the token measures. Furthermore he has to pay attention to the compliance with formalities and rules of health and safety measures as well as to the adherence to the instructions and if necessary give further instructions or interrupt the work.

After the conclusion of the work it has to be guaranteed, that the repaired work equipment is in a safe and functional condition and all work equipment and other utilities are removed. Where appropriate an inspection in regard to § 10 or the third paragraph of the BetrSichV is necessary.

After a done maintenance the testing has to ensure the safety of all those present. Not directly involved persons of the testing have to be kept away (barricade the areas). The procedure of the testing has to be determined. Before the beginning of the testing all employees have to be instructed about possible hazards and required protective measures (e.g. compliance of safety distances, usage of protective equipment) as well as measures for possible interruptions.

Hints from the VDI 2895 “Organization of maintenance:
The maintenance tasks can be divided into strategic and operative areas.

Area **SMS: Operational Control**

The **strategic area** includes the definition of maintenance goals (derived from the business goals), chosen maintenance strategies and organization.

The fundamental maintenance goal is to guarantee the required technical plant availability and safety. In addition there may exist a large number of goals, e.g.:

- systematic recognition of weak points in the plant
- implementation and documentation requirements by the authority
- cooperation with the plant manufacturers to work towards a suitable maintenance development

The maintenance goals can be retraced by indicators (maintenance indicator examples see VDI 2893 guideline).

A maintenance strategy indicates which maintenance measures have to be performed on which maintenance objects and at which date. General maintenance strategies are e.g. planned or failure-triggered maintenance strategy. The planned/ preventive maintenance is divided into:

- Predetermined maintenance which performs preventive maintenance work as scheduled (e.g. isochronous or after a fix number of utilization units) without the previous identification of the technical unit condition.
- Conditional maintenance with previous identification of the technical unit condition e.g. by inspection, measurement etc., to perform by means of the results necessary (preventive) maintenance work.

The criteria for the selection of the relevant maintenance strategy may be e.g. technical (e.g. wear behaviour), economical (e.g. remaining service life), safety-related/ legislative (e.g. deadlines), production relevant (e.g. technical availability) or object-specific (e.g. inspectability, predictability of failure performance).

The **operative maintenance area** includes maintenance planning, control, execution of measures and analysis.
Maintenance planning is the methodical preparation of all maintenance activities i.a. budget, personnel, equipment, workshop, material and work planning.
The results of work planning are work plans for the
execution of mostly scheduled (service plans, inspection plans) but also unscheduled maintenance measures (repair plans). A work plan contains, for example, the following for each maintenance activity:

- personnel, equipment and material requirements,
- type and sequence of the individual operations, planned times,
- health, safety and environmental regulations,
- protective measures,
- technical plans and drawings,
- checklists, etc.

It is pointed out to the VDI 2890 “Planned maintenance, Instruction on creating of maintenance lists”: The standard is intended to be a guideline for the use and design

of work plans and their integration into service/inspection plans and names necessary functionalities of computerised maintenance management systems (CMMSs).
In addition, the standard provides guidance on reviewing the plans over the life cycle of the item which is to be maintained.
Standardisation in creation of such plans is expected to improve communication with the manufacturer, integration into maintenance planning and control systems, and the incorporation of manufacturer's documents into an operation's maintenance manual.

The preventive maintenance works are terminated to e.g. minimize maintenance-induced production downtimes, to reach optimal utilization of the maintenance team's capacity as well as a demand-orientated coordination of all maintenance work.
Order monitoring is the process of continuously comparing the planned dates with the actual dates and capacities (utilization).

Maintenance analysis includes a retrospective, object- and activity-related evaluation, e.g.:

- planned/actual comparisons (costs and times)
- order deviation analysis
- weak points analysis
- damage cause analysis
- analysis of spares consumption

These data are used e. g. for determining defining system-specific indicator.

Total Productive Maintenance (TPM):
A concept developed in Japan based on an holistic systems approach in connection with the strategy of continuous improvement with the aim of eliminating all production losses and all wasting of resources, by:

- maintenance-friendly and low-maintenance design,preventive, conditional maintenance,
- systematic identification and evaluation of losses with the aim of permanent system improvement.

Hints:
There are maintenance concepts or maintenance systems that are based on a special principle e.g. commissioning principal, autonomous action of the competent department, necessity principal. A planned maintenance makes sense if the maintenance concept (Maintenance plan, handbook or similar) includes determinations to the following points: maintenance planning (strategy, personnel, material etc.), maintenance objects (plant components, equipment), maintenance measures (service, cleaning, inspection, repair).
Within the maintenance the responsibilities of all procedures have to be determined. The maintenance system can be IT-based and be located in a central organizational unit. Different plant components may have different service plans. Regulations for handling testing deadlines have to exist (see help to the question "How is the process for the guarantee of the proper implementation of (periodic) inspections evaluated?"

Area **SMS: Operational Control**

There may be criteria catalogues which specify which maintenance works can be done directly by the employees of the plant. The procedure for commissioning is regulated and the respective responsibilities and the handling of external companies is determined. The regulations for performing maintenance work can be different depending on the hazard potential, e.g. for a task with higher hazard potential there may be special permission systems.
There are determinations for the revision of the proper implementation of maintenance measures. On the basis of evaluations it is determined if the maintenance measures are implemented proper. The procedure for correction of the defects identified at the revision is determined. The responsible persons, the procedure and dates for revision, the derived measures and the evaluation of the implemented measures are defined. There are regulations for documentation in the scope of the maintenance process (e.g. content, participants, extend, storage time, access, initialization) and determined responsibilities for the (step-wise) documentation within the maintenance system such as documentation of identified failures in the performed revision.

Area **SMS: Operational Control**

Question 11: How is the process for the guarantee of the proper implementation of (periodic) inspections evaluated?

Help:
A special area of the maintenance is (periodic) inspections (see also help to the question „How is the Process for maintenance evaluated?"). At the (periodic) inspection the safety and performance of a technical unit gets evaluated by determined inspection methods, without further intended measures such as e.g. reparation. Depending on the test method appropriate measuring instruments are a prerequisite for the inspection. The aim at determining a deadline for periodic inspections is a safe usage and performance of a technical unit until the next determined inspection. The (periodic) inspections are regulated by law in the German Industrial Safety Regulation (Betriebssicherheitsverordnung (BetrSichV)) and the related technical rulebook, especially the TRBS 1201 "Prüfungen von Arbeitsmitteln und überwachungsbedürftigen Anlagen" ("inspection of work equipment and requiring supervision plants") or also

- TRBS 1201 Teil 1 Prüfung von Anlagen in explosionsgefährdeten Bereichen und Überprüfung von Arbeitsplätzen in explosionsgefährdeten Bereichen
  (Part 1 inspection of plants in explosive areas and inspection of the working environment in explosive areas)
- TRBS 1201 Teil 2 Prüfungen bei Gefährdungen durch Dampf und Druck (part 2 inspection of hazards from steam and pressure)
- etc.

Definition inspection in accordance to BetrSichV/ TRBS 1201: inspection of a test item includes the determination of the performance, target-performance comparison as well as the significance of the performance-target deviation.
In accordance to TRBS 1201 two review types are divided: organizational and technical reviews. The single reviews the review type, extend and dead-lines have to be determined as well as the necessary qualification of the review personnel.

The BetrSichV rules (excerpt of § 3 (6)): " the employer has to determine type and extent of necessary reviews of work equipment as well as the deadlines of periodical reviews, if this ordinance doesn't include corresponding specifications." "The deadlines have to be determined in a way that the work equipment can be used for sure until the next review."
Partially there are maximum deadlines in the BetrSichV that shall not be exceeded.

Plants that have special hazards such as fall/crash, explosion, fire or pressure are requiring supervision plants according to the BetrSichV. Besides the common regulation for work equipment requiring supervision plants additionally have to mind special regulations. Especially the inspections before commissioning as well as the periodic inspections of certain requiring supervision plants are demanded there. These plants shell only be used if the required inspections had been performed and documented. For special requiring supervision plants the inspection has to be done by the ap-

Area **SMS: Operational Control**

proved inspection agency. At the periodic inspections there have to be checked if the deadline for the next periodic inspection is correct.
The process for the guarantee of the proper implementation of (periodic) inspections has to be part of the SMS either in an independent process or integrated in the process “maintenance”.

The process sequence has to ensure that all safety related parts in terms of plant/ proses safety are identified, that they are necessary for the periodic inspection and deadlines are determined. Inspection deadlines have to be established by criteria (regulations, malfunction data etc.). The criteria have to be questioned at definite dates (regular inspections, influence of new findings, incidents). The observance of a time limit and the correct implementation of the inspections have to be guaranteed.
The responsibilities for all tasks in the process sequence as well as the documentation have to be defined. The fulfilment of the requirements of the BetrSichV has to be guaranteed.

Area **SMS: Operational Control**

Question 12: How are the regulations for the management and control of risks associates with ageing equipment evaluated?

Help:
The ageing of plants and plant parts can be prevented by a good maintenance and (periodic) inspections. The maintenance serves as the conservation of the safe plant and plant part conditions and includes all measures therefore especially inspection, service and repair as well as (periodic) inspections. At the (periodic) inspection the safety and performance is checked by determined inspection methods with the aim to guarantee a safe usage and performance until the next periodic inspection. If there isn't a guarantee further (maintenance) measures are made such as e.g. repair, replacement etc.

According to MAHBulletin Lessons Learned No. 7 „Major accidents related to ageing" the preventive handling with ageing of plants and plant parts should include the following points:

a. physical material ageing of the plant components
b. Ageing by changes due to new technologies
c. Ageing by design change due to organization, management and human factor
d. Ageing by conceptual enhancements of the safety philosophy, Change in engineer standards and other regulations.

The points above are covered in large part by processes that are requested in other areas. At the Inspection the focus is the aspect ageing. This aspect is part of the following questions:

Area SMS: Audit and Review:

- How is the procedure of the systematic review and evaluation of the SMS (management review) evaluated?
- How is the safety culture of the establishment valued?

Area SMS: Monitoring Performance:

- How is the process of the audit system evaluated?
- How is the process "internal reporting system" or the regulations of registration and handling of incidents evaluated?
- How are the regulations for using safety performance indicators in the plant and process safety evaluated?

To a) physical material ageing of the plant components:
From the area SMS: Operational Control:
How is the Process for maintenance evaluated?
How is the process for the guarantee of the proper implementation of (periodic) inspections evaluated?

Area **SMS: Operational Control**

From the area SMS: Identification and evaluation of major hazards:
How is the process of identification and assessment of major accidents being evaluated?
How are the applied systematic methods being evaluated?
How are the procedures for the determination and definition of the safety relevant parts of the establishments being evaluated?
How are the procedures for the determination and fixing of the safety-related parts of the plants within the Establishment being evaluated?

To b)/d) "Ageing by design changes due to new technologies"
From the area SMS: Operational Control:
How is the process for the guarantee of the proper implementation of (periodic) inspections evaluated?
From the area SMS: Management of Change (MoC):
How is the management of change (MoC) being evaluated?

To c) Ageing by design change due to organization, management and human factor:
From the area SMS: Organisation and personnel:
How is the process knowledge management evaluated?
From the area SMS: Management of Change (MoC):
How is the management of change (MoC) being evaluated?
How is the scheme to ensure the completeness and updating of the operating documentation being evaluated?

Hints for inspectors:
Possible questions to the aspect ageing:

- Are there any specifications in the establishment how the material ageing of plant components is considered?
- Are there any indicators to evaluate ageing?
- Which indicators are used?
- Which specifications are there in the establishment if there are changes in the state of the art, especially
  - in the spare part management of old components
  - to guarantee the compatibility of old and new technologies
- How the knowledge transfer is guaranteed if there are changes in personnel in the areas management / organization?
- Which specifications are there towards conceptual trainings of the safety philosophy or the implementation of changes in engineer standards or other regulations?

The following documents (process description, management instruction) should be examined in particular:

- Maintenance and periodic inspections
- MoC-Process
- Documentation control and operating documents

Area **SMS: Operational Control**

- Knowledge management
- Qualification of the employees
- Identification and evaluation of major hazards

It should be focused on the document's aspects of ageing. In what extend is it considered? Further-more to the PDCA-cycle, that means there have to be regular reviews if the determined contents for the documented process (i.e. process, responsibilities) are appropriate , e.g. in the scope of audits.
The usage of indicators in the establishment for the evaluation of the plant/plant part ageing conditions is seen positive.

For **further hints and explanations** see OECD-publication "Ageing of Hazardous Installations", March 2017

Great Britain focused 2010 the aspect ageing at inspections of establishments.
In the scope of this the HSE (Health and Safety Executive) published different documents, e.g.:

- Managing Ageing Plant – A Summary Guide
- Ageing Plant Operational Delivery Guide of the COMAH Competent Authority

The last is an authority guideline for the inspection of ageing plants. The Annex 5 includes the following 7 inspection elements with questions:

- Topic 1: Leadership
- Topic 2: Plant and equipment on site – the Asset Register
- Topic 3: Assuring the integrity of the primary containment boundary
- Topic 4: Assuring the integrity of safety-critical mechanical equipment
- Topic 5: EC&I Inspection and Test
- Topic 6: EC&I management of Out-of-date or Obsolescent Equipment
- Topic 7: Resources

In both HSE publications it is pointed out that ageing is not only a reason of years in service but also a reason of the plant condition (loads and changes of the plant). The condition of the plant must guarantee a failure-free production. This can also be fulfilled by very old plants, while backwards a relative "young" plant may have strong signs of wear that may be followed by a failure of equipment accessories with serious dimensions. The last should be prevented by measures- the focus lays on the maintenance measures and periodic inspections.

The HSE-publication „Manageing Ageing Plant – A Summary Guide" mentions as an important elements for a safe behaviour in case of plant ageing:

- Maintenance Management Systems
- Asset Management and Integrity Systems
- Audit and Inspection regimes
- Risk Assessment Management processes
- Management of Change procedures
- Permit to Work

Area **SMS: Operational Control**

- Responsibilities and Communications
- Training and Competence development

As possible indicators for the evaluation of the ageing condition the HSE-publication mentions:

Leading Indicators

- Number of planned inspections
- Number and frequency of audits
- Planned replacement schedules for plant and equipment
- Number of Emergency Response exercises planned
- Planned number of tests done on safety critical equipment
- Training plans for identified staff and staff numbers attending
- Planned procedure reviews

Lagging indicators

- Number of major failures of plant and equipment
- Number of uncontrolled releases of product
- Number of reworks to maintenance activities
- Number of outstanding audit/Inspection action items
- Number of alarm/instrument failures during testing
- Number of incidents when working under a Permit to Work system
- Number of incidents due to Human Error

Question 13: How are the regulations towards procurement of materials and equipment evaluated?

Help:
It is necessary that the aspects of plant and process safety figure prominently at purchases. Rules and criteria to ensure this must exist and be followed (examples are criteria for selecting suppliers and appraising their qualifications, testing the possibly dangerous properties of chemicals before they are purchased and handled, handling of hazardous chemicals only when delivered with safety data sheet according to the guidelines of the European Union, use of materials and equipment with directives for testing them).

Area **SMS: Management of Change (MoC)**

Area

SMS: Management of Change (MoC)

Question 1: How is the management of change (MoC) being evaluated?

Help:
Changes in an operating area can occur planned or creeping, and may affect technical, organizational or management relevant aspects of an Establishment. For the accident prevention according to the German Major Accident Ordination a comprehensive understanding of the importance of change is important.
Monitoring and an efficient SMS in combination with a good safety culture are necessary to prevent safety-relevant consequences of creeping changes, which are difficult to detect elsewhere.
For the safe execution of planned changes, it is important to determine whether these have an impact on the implemented safety concept. This requires an overview of the consequences of the change.
Therefore, planned changes are made in the context of the process for the secure execution of changes (Management of Change: MoC). For each establishment this is specified in writing in, e.g. in the form of a process description / process description / management instruction, etc. The following aspects must be taken into account:

1. Objectives which should be implemented and achieved with the MoC process (e.g., secure implementation of planned changes, effective use of investments),
2. Scope (for example, establishment, types of changes, organizational units of the operating area, equipment),
3. Definition of terms (in particular changes relevant to safety, gradation of modifications),
4. Description of the process steps and sequence of the MoC
5. Definition of the contents of the process steps and tasks (start-up and shutdown processes, emptying and cleaning of plant parts, standstills, effects of construction and storage activities (for example, accessibility for Firefighters)
6. Definition of the Chain of Command and responsibilities for the process steps and tasks,
7. Consideration to the interfaces of other processes (e.g., risk analysis, need for authorization, documentation, operational control, emergency planning, audit system),
8. Definition of documentation (content) during the process steps.

Periodic verifications must be carried out to determine whether the defined content is appropriate for the MoC process (including criteria, work flow, responsibilities), e.g. in the context of audits.

The considerations above apply to medium-sized and large companies. Small businesses must write down their procedures and criteria, taking into account the re-

quirements of the German Ordinance on Major Accidents. Because of the other organizational structure, this can take place by adding a chapter to the management manual.

The procedure for changes must be checked regularly. Criteria must be laid down for this purpose (for example, time intervals, consideration of special occasions (for example, accidents or near misses; criteria to check what, when, how, by whom (for example, completeness of all safety-related aspects, consideration of new findings, etc.). The responsibilities for this must be clearly defined. Regulations for the documentation and handling of the results from the verifications must exist.

References to the above-mentioned points, e.g. procedural instruction:
There are written procedures how changes are made (investments, repairs) in the establishment. Changes in process procedures with investment requirements generally require the assessment and approval of various departments in the establishment / company.

They should permit an integration of plant and process safety matters early on.

The procedures may comprise elements such as descriptions (e.g. application for implementation of a change, expertise, approval by experts, start-up operations), reasons, required funding, documentation, checks. All persons responsible for the respective steps in the event of a change shall be specified in writing.

Generally, there will be subdivisions among the procedures involved in the change, e.g.

- changes planned in the long-term (new plant / maintenance),
- changes necessary in the short term due to special circumstances,
- safety relevance / importance to plant and process safety,

The company-internal release process of an amendment should be designed in such a way that the project itself - as well as the decision about it- is transparent. It should also offset the reason for a possible rejection.

The modification procedures may be dependent on the safety relevance in view of the complexity of the various steps, for example they may depend on:

- Preparation,
- release,
- implementation of the amendment,
- verification of the change,
- documentation,

Criteria should be provided for determining safety relevance, e.g.

- extent of the changes,
- affected parts (for example with / without dangerous substances),

Area **SMS: Management of Change (MoC)**

- change of chemical reactions (includes, for example, the change in the order of substances (substance mixture) and should, in principle, not be carried out without the relevant safety-related characteristics)
- Definition of alterations of different safety relevance (for example, building painting, replacement of a production container).

Even changes with low importance to plant and process safety may nevertheless have an influence on the safety concept of the installation or the establishment as well.
Also, it is important to check the possible effects on connected systems (e.g. supply of nitrogen, power supply, emergency plans, and transportation).
The connection with rules concerning determination and assessment of hazard potentials needs to be defined clearly (e.g. based on the amounts of substances or changes in the process procedure). Those responsible for compliance and updating of the criteria need to be appointed.

Area **SMS: Management of Change (MoC)**

Question 2: How are the regulations for communication at the different stages of a Management of Change (MoC) evaluated?

Help:
There are rules that regulate which company expert divisions are involved in changes (how, when, who, why) and also how it is guaranteed that all persons/divisions involved in the planning phase of the modification have access to all safety relevant data (e.g. transfer documents, hand-over communication etc.).

It is required that the staff is informed about the changes in time (the time chosen for informing the staff depends on the extent, type of change or the impact caused by the change). Instructions on the extent, content and mode of the information passed on to the staff should be fixed. It may be done in writing in simple language that is easy to comprehend and should contain the changes as well as the effects of the changes on the various operations (process operations, maintenance, repair, etc.). In addition, it is important to tune the operating manual and the documentation on the installation to the changes. Those responsible for passing on the information need to be appointed.

Periodic checks of the information flow and of how the results coming out of it are handled are necessary. This can be done within the framework of the audit system.

Area **SMS: Management of Change (MoC)**

Question 3: How is the scheme to ensure the completeness and updating of the operating documentation being evaluated?

Help:
Procedures need to be set which make sure that the documentation on the modification process is updated (e.g. in phases if necessary).They address the comprehensive and complete documentation of the changes and of updating all documents affected by the change. The responsibilities for this must be clearly defined. A periodic check of the procedures is necessary. All relevant safety guidelines and operating instructions and other manuals are always kept up to date.
Changes to the plant must be transferred to the R&I-flow charts. The installation documentation as well as the safety report had to be adapted. It is referred to the consideration of documentation change in the framework of necessary notification and approval procedure.
Rules for the verification process, whether the updating of the documentation was done properly and completely, must exist. This can be done within the framework of the audit system.

One way of checking entire compatibility is to compile an installation or operating manual which contains all documents (from the first draft of the plan to the licensing document, from the safety report for the installation to the documentation of the maintenance work performed and the safety engineering modifications as well as the extensions of the installation, etc.). All documents should be up to date. All documentation concerning a process from the research phase on also belongs to the manual and should be kept up to date. The comparison of the data in both documentation enables a meaningful compatibility check possible. For this regulation too, jurisdiction must be clearly defined.

Area **SMS: Management of Change (MoC)**

Question 4: How are the regulations for a temporary shutdown of a plant in the establishment being evaluated?

Help:
Provisions on the procedure and responsibilities for a standstill of an installation or the shutting down thereof must be present. This also includes regulations for the release of hazardous substances or pressures, cleaning, securing, dismantling, acceptance and documentation.

Definitions for archiving the system documentation may be required.

Rules for the verification process, whether standstills are carried out properly, must exist. This can be done within the framework of the audit system.

Question 5: How are the regulations for start-up a plant in the establishment being evaluated?

Help:
Rules for procedures of start-up operations including the rules for final inspection and acceptance and for documentation need to exist and those responsible for it need to be appointed. It may be advisable to include rules to determine the persons/company expert divisions/external companies that are to be involved in the process of taking into operation and also which documents on the installation need to be handed over.

Rules for conducting the exchange of experience between the personnel involved before the hand-over of the installation and the personnel in charge of the operation of the installation should be available. This exchange of experience should continue for a certain period of time, e.g. during the first year of operation.

Rules for checking whether the installation was properly taken into operation needs to exist. This can be done within the framework of the auditing system.

Area **SMS: Planning for emergencies**

Area

SMS: Planning for emergencies

Question 1: How are the regulations towards the process information to the public evaluated?

Help:
Since 2017 the information to the public is obligatory for the operator of an upper-tier as well as lower-tier establishment. This is regulated in § 8a "Information to the public" of the German Major Accidents Ordinance in conjunction with annex V part 1: Information about lower-tier and upper-tier establishments.
There are further requirements for upper-tier establishments in § 11 „Weitergehende Information der Öffentlichkeit“ and Annex V part 2 “ Weitergehende Informationen zu Betriebsbereichen der oberen Klasse“ that have to be fulfilled.
The operator has to determine in writing the procedure of preparation, distribution and actualization of the documents for information to the public.

In small companies this can be realized e.g. in a chapter of the management handbook.

For middle sized and big companies the process “information to the public” should be documented in the form of procedure/ process descriptions/ management instruction etc. The documentation has to be determined in writing and should include the following points:

- Aims that should be implemented and reached
- Application range
- Definitions
- Description of the process steps and procedure of information to the public
- Determination of the process step and tasks
- Determination of task competences and responsibilities
- Consideration of process interfaces (e.g. hazard analysis, identification and evaluation of hazards at major accidents, audit system)
- Determination of the process step documentation contents

Regular reviews have to be done to evaluate the contents of the process information to the public. This can be realized e.g. in audits.

Further hints and contents

For the implementation of the information to the public counts:

- the details for information to the public have to be up to date, and be accessible permanently, also electronic
- the details have to be published (for the first time) one month before putting into service of an establishment as well as

Area **SMS: Planning for emergencies**

- one month before major accident related modifications according § 3, paragraph 5b German BImSchG

In accordance to Annex V part 1 of the German Major Accidence Ordinance the information to the public must include the following details:

1. Name or company of the operator and the complete address of the establishment.
2. a) A certification that it is an upper-tier or lower-tier establishment according to German Major Accidents Ordinance and it is notified to the supervisory authority according to § 7.
2. b) The safety report according to § 9 is submitted to the supervisory authority if it is a upper-tier establishment.
3. An understandable formulated explanation of the establishment operations.
4. Mention of relevant dangerous substances in the establishment, which could cause a major accident. The substances must be mentioned in a common or generic nomenclature or hazard classification as well as the hazard properties in general parlance.
5. a) General information about how the affected population is warned.
5. b) Adequate information about the behaviour in case of a major accident.
6. a) Date of the on-site survey in the framework of an inspection according to § 17 by the competent surveillance authority.
6. b) Briefing where to find detailed information on request about the on-site survey and about the inspection plan according to § 17.
7. Details where to find more information.

to 5.b), 6.a): Alternatively there could be a hint where this information can be found in electronic form.

It is possible that the operator limits the information to the public for reasons of public or private interest protection. This requires the approval of the competent authority according to the regulations of federal and federal state about access to environmental information.

The operator of an upper-tier establishment has to make the safety report on request accessible to the public immediately, according to § 9.
After the approval of the competent authority the operator is allowed to create a version of the safety report where some parts are not externalized and to make this version accessible to the public.

The operators of “domino-establishments” according to § 15 German Major Accidents Ordinance have to cooperate towards the information to the public (§ 6, paragraph (2) Major Accidents Ordinance).

The information must be made accessible to the public. This has to be done electronically e.g. in the internet. In addition it can be done e.g. by a display board or information brochures that are deposited at the gate.

Area **SMS: Planning for emergencies**

In case of a lower-tier establishment the suitable or respectable distance according to KAS-Leitfaden Nr. 18 can be the indication for the radius of in-formation brochure distribution.

Further requirements for upper-tier establishments according to § 11 and Annex V part 2:

a. The information to the public has to include extra details according to Annex V part 2.
b. b. The operator of an establishment has to inform adequately all persons and all operating sites or neighbouring establishments that may be affected by a major accident in the establishment before putting into service about the safety measures and the right behaviour in the case of a major accident. This can be realized by information brochures that are distributed to the addresses in the affected range of a potential major accident. The possible affected range of an establishment plant results from an atmospheric dispersion modelling of an anyhow-major-accident. The information brochure includes at least the details of Annex V. The distribution of this brochure has to be made regularly but not less than every 5 years.
c. The information has to be coordinated with the emergency management and hazard control authority.
d. The operator has to evaluate the information according to b.
    - At least every 3 years and
    - At a major accident related modification according to § 3 paragraph 5b German BImSchG.
e. If there are changes at the evaluation that may have serious effects on the major accident related hazards, the operator has to actualize the information and repeat b.

Part 2 of Annex V “Further information to the upper-tier establishments” includes the following requirements to the content of the information to the public:

1. General information towards hazards, which arise of a major accident, including possible effects to human health and the environment and a summarized Information of the major accident scenarios and measures with witch these scenarios can be prevented or the effects can be limited.
2. A confirmation, that the operator is obligated to take suitable measures on the ground of the establishment to combat major accidents and to limit the effects of a major accident at its best – also in cooperation with emergency and rescue service.
3. Appropriate information from the external emergency plans to combat the effects of incidents outside of the establishment with the order to obey the requirements of emergency and rescue services in the case of an incidents.
4. If necessary, specifications if an establishment is near to the territory of another member state and there is a possibility that the major accident may have cross-border effects according to the Convention on the Transboundary Effects of Industrial Accidents (UNECE).

Area **SMS: Planning for emergencies**

An adequate information towards the potentially nevertheless occurring emergency situation is important to prevent misbehaviour of the general public or to perform an evacuation quickly if necessary. Criteria for the information to the public must exist. Two aspects can be differed: On the one hand the previous information to the public according to §8a and 11 of the German Major Accidents Ordinance, Annex I, and on the other hand the information path at an accident between operator, competent authority and the public. This is regulated in the emergency planning.
The responsibilities of the particular points have to be regulated clearly in the establishment. This also counts for the configuration of interfaces to the external hazard control.
Reviews of the points above have to be done. Important is also a regular review of the information towards being up-to-date and how the information is received in the public (are all households reached, is the information understandable). The implementation of measures because of the review results has to be checked. The responsibilities therefor have to be determined.

Area **SMS: Planning for emergencies**

Question 2: How are the regulations towards the process planning for emergencies evaluated?

Help:
The emergency planning serves to the preparation in advance by the operator of an establishment, how in emergency case should be proceeded, that the effects of a major accident or serious accidents can be limited as far as possible.
Therefore there has to be a systematic investigation which emergency cases can occur and which reaction is appropriate in an emergency case.
In emergency case there have to be determined organization and task arrangements and clear rules for actions and behaviour in emergency case. These rules apply equally to all establishments.

At middle sized and big companies the process “planning for emergencies” should be documented in the form of procedure/ process descriptions/ management instruction etc. The documentation has to include:

- Aims
- Application range (establishment, if necessary step-wise e.g. organization units of the establishment, plant)
- Definitions
- Description of the process steps
    - Preparation of (internal) emergency plans as well as further emergency documents
    - Trainings
    - Emergency exercises
    - Notification requirement
    - hazard control workforce
    - crisis management group
    - Information, coordination and cooperation with external crisis management organizations
    - Information, coordination and cooperation with external e.g. neighbouring establishments
    - Information of affected population and sensible institutions
    - Identification and provision of necessary safety equipment/ operating re-sources/communication equipment for the employees/ relief units/ crisis management group
- Determination of the process step and task contents
- Determination of task competences and responsibilities
- Consideration of process interfaces (e.g. education, identification and evaluation of hazards at major accidents, internal re-porting system),
- Determination of the process step documentation contents

Regular reviews have to be done to evaluate the contents of the process personnel planning (i. a. process, responsibilities, contents, interfaces).This can be realized e.g. in audits.

Area **SMS: Planning for emergencies**

The operators of a “domino establishments” according to § 15 German Major Accidents Ordinance have to exchange as per § 6 Major Accidents Ordinance all significant information to take account in the internal emergency plan of the type and extend of the all-over hazard as well as to cooperate with the competent authorities at the transfer of information on the preparation of the external emergency plan. The responsibilities in the case of cooperation, exchange and identification, configuration and transfer of this information have to be defined. A regular review and if necessary actualization has to be guaranteed.

Further hints
A very important element of emergency planning is the internal reporting sequence, which includes all relevant reporting trails and their trigger criteria. The reporting trails have to be prepared and defined e.g. in form of alerting scheme, telephone, reporting and alerting lists. All developed documents have a determined review and actualization procedure, up-to-dateness of the emergency phone numbers in particular.
An example for the design of an (external) reporting sequence is an agreement of a stepwise reporting system of first-of-all reports to the hazard control authority as it is shown in Annex 3 of the “Vollzugshilfe zur Störfallverordnung”.

A procedure for the protection of external employees must exist. Therefore a stepwise concept can be used (e.g. visitors are escorted by the establishment employees, if necessary an instruction into the safety measures of the shown areas is done, instructions for employees of the external services etc.) It has to be guaranteed, that there is an easy control of the number of people located at the plant in the establishment. This can be realized e.g. in a registration card system.

Explanations from the KAS-Leitfaden Nr. 29:
For the Implementation of appropriate statutory rules (i. a. German Major Accidents Ordinance) and for prevention of an emergency case it is recommended to assign the following tasks to a specific position, to practice preventively and to review. These should also be documented in the framework of the emergency management and preceded in case of emergency:

- Conceptual and editorial processing of the emergency plans
- Preparation and update of the necessary practical and legal regulations for the relevant location
- Implementation of revisionary legal frameworks at the location
- Organization and supervision of the major accident central office, setting of a crisis management group
- Organization of the inter- and corporate-divisional location preparedness
- Coordination of the damage management procedure of all employees and a guarantee of an organized communication with the authority, neighbourhood and press.
- Reprocessing of the reasons for incident.

During an emergency case intransparency, dynamic and uncertainty of a situation may necessitate a switch in the strategy instead of being forced on a rash acting. If

there is an acute need for acting at first an option should be chose which improves the safety situation and increases the time slot (no-regret-decision). This switch can be realized by a person, which can to some extend be outside of this situation and acting (e.g. special emergency manager, member of the operation controllers, operations manager of a neighbour establishment).
There has to be a special attention on a wise task allocation of the personnel for the case of emergency.
Convenient is if the involved persons know each other from teamwork because then they can develop a shared knowledge (knowledge of the group members such as competences, tasks, responsibilities. This is a development of teamwork).

In preparation for the emergency case the existing items of equipment and tools have to be checked critically.
Because the emergency case is normally seen as a stressful situation all aspects should be limited that require additional mental capacities, e.g. by an ergonomic display design.

Further Hints:
Regulations for the preparation and update of the emergency planning have to exist. There could be criteria for gradations (e.g. internal emergency plan according to §10 German Major Accidents Ordinance, plant alerting plans, alerting order of administration building, cafeteria etc.) which concern e.g. content, extent (preferred short, clear and succinct), documentation, distribution, deadlines, instructions. See “Vollzugshilfe zur Störfallverordnung” as a source of knowledge.
The preparation of necessary resources and tools has to be guaranteed. Involved persons and positions have to be defined. It is useful to participate the employees in the emergency planning or mandatory at application of §10 German Major Accidents Ordinance. The responsibilities of emergency planning preparation and update as well as the preparation of resources have to be regulated clearly.
Defined criteria for the scenario taken as a basis can be useful. The interfaces to area SMS: “Identification and evaluation of major hazards” are clearly defined.
Regulations and responsibilities for a regular review of all points named above and the update of emergency planning must exist. The emergency planning has to be checked and be evaluated and if necessary updated after every plant modification. The procedure of the update has to be reviewed. Changes have to be documented for a better reproducibility (interface to “control of documents”).

Area **SMS: Planning for emergencies**

Question 3: How are the regulations towards the process preparation and review of documents for emergency planning evaluated?

Help:
At middle sized and big companies the process "preparation and review of documents for emergency planning" should be documented in the form of procedure/ process descriptions/ management instruction etc. There may be an interface to the process "control of documents".
The documentation has to include:

- Aims
- Application range
- Definitions
- Description of the process steps and procedure, preparation and review of
  - emergency plans
  - alerting scheme
  - telephone, reporting and alerting lists
  - further emergency documents,
  - Information for the external crisis management
  - etc.
- Determination of the process step and tasks
- Determination of task competences and responsibilities
- Consideration of process interfaces (e.g. personal and organization, identification and evaluation of hazards at major accidents, internal reporting system, audit system)
- Determination of the process step documentation contents

Regular reviews have to be done to evaluate the contents of the process named above (i. a. process, responsibilities, contents, interfaces).This can be realized e.g. in audits.

The information flow in the case of emergency has to be defined clearly in the scope of emergency planning.

Hints to the points above e.g. procedure description:
According to Annex IV of the German Major Accidents Ordinance the emergency plan, which has to be done obligatory by the operators of an upper-tier establishments, has to include the following information:

1. Name or operating position of the person which is authorized towards the introduction of immediate measures, as well as the person which is responsible for the implementation and coordination of remedial measures on the establishment area.
2. Name or operating position of the person which is responsible for the connection to the competent authority for external emergency plans.
3. at predictable circumstances or incidents which can be decisive for triggering the major accident, in each individual case a description of measures that

have to be taken to control these circumstances/ incidents and to limit the effects as well as a description of the safety equipment and operating resources.

4. Preventions towards risk limitation for personnel in the area of the establishment, information towards the alerting type as well as the expected behaviour of the persons in case of an alert.
5. Preventions towards early warning of the competent authorities which is responsible for the introduction of in the external emergency plan provided measures. The type of information, which has to be communicated at the first notification as well as preventions for the transfer of detailed information as soon as they are available.
6. Preventions towards education and training of the personnel in tasks which performance is expected as well as coordination of this education/training with external emergency and rescue services.
7. Preventions towards the support of remedial measures outside of the establishment area.

According to § 10 German Major Accidents Ordinance the employees have to be involved in the preparation of an internal emergency plan as well as in the regular review of the emergency plan (at least every 3 years) or occasion related and if necessary update them immediately.

Criteria for an occasion related review may be:

- Incident
- Knowledge from the emergency training
- New technical knowledge and knowledge about acting in case of major accident
- Modifications in the establishment: organizational, technical, management specific type
- (safety relevant) Plant modification
- Modification of internal crises management
- Modified specifications
- Modified requirements or resources at the external crises management, relief organizations and institutions
- Changed address/ telephone numbers

Hints from the "KAS-Leitfaden Nr. 19:
The preparation of the emergency plan according to § 10 and Annex IV of the Major Accidents Ordinance is only binding for upper-tier establishments. At a lower-tier establishment some minimum standards according to the regulations:

- preparation of escape and rescue plans
- preparation of fire brigade plans, see DIN 14095
- application of BGV A1 (UVV Grundsätze der Prävention), e.g. measures at special hazards, first aid, personal protective equipment
- operating instruction according to § 14 German GefStoffV, i.a. with information on measures, that have to be done by the employees, especially of the rescue

team in case of interruption, accidents, emergency and prevention of these cases.

It makes sense to have available the emergency numbers and a preparation of the notification system, if necessary the implementation of an on-call duty as well as regulations for decision-making authority for emergency cases. All documents have to be subject to a fixed review and updating procedure.

With regard to emergency situations all work instructions should include the following requirements (KAS-Leitfaden Nr. 29):

- Information should be classified towards the type such as requirements, operation steps etc.
- The necessary action steps should be documented in short numbered lists in dependence to the performed process e.g. 1. Open valve xy 2. Open valve yz NOT 1. Open valve yz after you already opened valve xy.
- An action step should begin with a verb and only a single action should be mentioned. action steps should be named precisely and clearly, wordings such as “approximately” or “adequate” shouldn’t be used.
- The employees shouldn’t do mental operations such as mental arithmetic or written addition.
- Warnings or safety requirements should be highlighted.
- The text should be structured by clear headlines.
- Passive voice and double negative should be avoided.
- The linguistic usage should be consistent fitted to the operator. If abbreviation or special technical terms are used, they must be explained and used in all documents consistently.

The attention handling of operation steps can facilitate if necessary by checklists witch have to be prepared. Instructions for emergency should be short, precise and easy to understand as well as be limited to the essentials. It is helpful to have these readily available in form of a hardcopy for typical default scenarios such as electricity or cooling.

At the planning it should be considered if in an emergency situation if necessary different tasks should be operated by several people at the same time. If this is the case, operation instructions have to be available in an equivalent number.
Furthermore it has to be checked if single action steps have to be performed at remote places. There have to be instructions on site or the relevant pages should be available to take away. If tools, components or plant sections have to be used, that aren’t part of the daily work, illustrations in the instructions are a good possibility to support the acting person. Keeping telephone, notifying and alerting lists up to date is absolutely necessary.

Area **SMS: Planning for emergencies**

Question 4: How are the regulations towards the process of emergency trainings and emergency plan testing evaluated?

Help:
Because the emergency situation differs basically from the normal situation, preparations in the form of regular instructions education and exercises are mandatory. Regulations for the process “instruction/education/exercises in case of emergency” concern the employees of the establishment as well as external employees or organizations (e.g. the fire department) and include also the implementation of the emergency exercises, emergency plan testing or the operation of a crisis management group.

At middle sized and big companies the process “instruction/education/exercises in case of emergency” should be documented in the form of procedure/ process descriptions/ management instruction etc. there may be an interface to the process “familiarization, qualification/ further education of the employees”.
The documentation has to include the following points, these may already be covered partially in the process “familiarization, qualification/ further education of the employees”:

- Aims witch should be reached with the process “instruction/ education/ exercises in case of emergency” (e.g. effective action in the case of emergency, regular participation of the establishment employees)
- Application range (e.g. establishment, organization units of the establishment, plant shift, visitors, external employees)
- Definitions
- Description of the process steps and procedure (qualification measures: instruction/education/exercises plans and their contents, the implementation and analysis of the performed qualification measures, dates for the implementation of qualification measures (interval (instruction and testing of emergency plans: at least every 3 years), occasion-related etc.))
- Determination of the process step and tasks (instruction and testing of emergency plans, type of the exercises, group of people to be included (employees of the establishment, external employees external assistance organization and emergency), danger prevention organization) analysis of qualification measures experience, implementation of the measures from the analysis)
- Determination of task competences and responsibilities
- Consideration of process interfaces (e.g. personal and organization, identification and evaluation of hazards at major accidents, internal reporting system, audit system)
- Determination of the process step documentation contents

Regular reviews have to be done to evaluate the contents of the process named above (i. a. process, responsibilities, contents, interfaces).This can be realized e.g. in audits.

Area **SMS: Planning for emergencies**

The instruction contents in particular guarantee the complete knowledge about the necessary ways for notification and their trigger criteria.

There have to be reviews that also analyse if the instructions about relevant content of the behaviour in case of emergency are communicated appropriately and are understood by the instructed persons. The responsibilities have to be defined.

Instructions of new employees about the contents of the emergency planning have to be done at the beginning of their new task. According to §10 (3) of the German Major Accidents Ordinance the instruction has to be done before starting the employment and also counts for external personnel, also not temporary external employees.
These contents of emergency planning can be integrated in the framework of the regulations towards familiarization (interface to the Area SMS: Organization and personnel).

A procedure for the protection of external employees in the case of emergency has to exist. Therefore a stepwise concept can be realized (e.g. visitors are accompanied by an employee of the establishment, if necessary an instruction towards safety in the visited units is performed, instruction of external employees etc.) It has to be guaranteed that a simple control is given to know how many people are in the plant / establishment area. This can be realized in a registration card system.
For the instruction of external employees there may be an interface to the area SMS: Operational Control or the instruction towards the behaviour in the case of emergency can be integrated in the safety instruction.

Hints to the points above e.g. procedure description:

Elements from the KAS-Leitfaden 29:
During the handling of emergency situations not only cognitions (e.g. thinking or knowledge) play a role but also emotions (e.g. fear) and acting motivation (rescue of one's own).
The transfer of necessary competences for emergency situations should be realized in employees training sessions. Trainings for not-projectable situations should include the following contents:

- Team building and maintenance of team operational capability also at strong pressure action and failure
- Procedure for decisions at insecurity and pressure of time (e.g. FORDEC)
- Leadership behaviour in the critical situation, flexible handling of leadership requirements
- Knowledge of typical failures and snares at acting under indecisiveness and shortage of time such as limited hypothesis formation, neglect of action control
- Knowledge of the mechanisms (and failure tendencies) at situation rating on condition of insufficient and unreliable information and methods of constructive handling with informational overload
- Understanding of individual reaction patterns in case of stress and emotional distress as well as stress reduction
- Methods for the development of a common situation perception

Area **SMS: Planning for emergencies**

The contents of the trainings should be deepened in simulations of emergency situation.

Types of trainings may be:

- Alerting training
- Training to increase the clarity of messages
- Plan discussion/plan training
- Staff training
- Crises management training
- Staff framework training
- Strategic crises management group training
- Trainings for sub-functions
- Complete trainings/ simulations

Also possible is the use of virtual reality for accident simulators, which can be used for the emergency training by the employees of the establishment in conjunction with the simulator of the process control system. Also useful are media trainings with the members of the crises management group.

Also small and medium sized companies are recommended to perform trainings with the local fire brigade, the authority and the police.

Area **SMS: Planning for emergencies**

Question 5: How are the regulations towards the establishment's authority to decide in emergency case evaluated?

Help:
It is pointed out to § 12 (1) No. 2 of the German Major Accidents Ordinance, where the operator of an upper-tier establishment has to name an authorized person to the competent authority that is responsible for limiting the effects of major accidents.

Who and when a decision is made, if the planning for the case of emergency has to be implemented should be located preferably high in the company hierarchy and should be defined with definite criteria in cooperation with safety responsible person (e.g. major accident commissioner/ safety apartment/ plant management). Criteria that may play a role are in particular the time factor as well as authorities, competences and the appropriate acceptance of responsibility of the position by the person who makes the decisions or implements them.
Positive seen are clear stepwise appropriate authorities to decide, which i.e. begin with definitions in the plant operating instructions at which alerting value the management has to be informed or at which alerting value the management has to decide about the measures to be initialized.
The up-to-dateness has to be guaranteed and has to be reviewed regularly.

Elements from the KAS-Leitfaden 29:
If emergency situations have to be handled decisions have to be made under a high insecurity and pressure of time. Wrong decisions can cause disastrous consequences. The FORDEC-method was developed for pilots to be able to make structural decisions in critical situations. This method can be used analogical for emergency situation in technical plants. Decisions should get more robust towards rash and not appropriate impulses and emotional impacts and have to be trained in qualification measures.
Also during the emergency situation intransparence, dynamic, and insecurity of the situation may need a rethinking of the strategy, instead of forcing a rash action. For example, if an acute pressure of action occurs, at first an option has to be chosen that improves the safety situation and if possible brings more time buffer (no-regret-decisions). This switching can be made most likely by a person who is, in a sense, beyond the happening and action (e.g. special emergency manager, member of the operations management, operation manager of a neighbouring establishment).

The information flow in an alarm or emergency situation has to be defined clearly in the context of the emergency planning.

The integration of the responsible person for safety in an alarm situation has to be determined.

The responsible persons for safety have to be informed directly and totally. Total information can be reached by accident/major accident sheet. (an interface to the area "SMS: Monitoring Performance" particulary help to question "How is the process "in-

Area **SMS: Planning for emergencies**

ternal reporting system" or regulations of registration and handling of incidents evaluated?" may exist.) The content of the sheet could be: exact place of the incident, number of injured person, type of damage, extent, involved substances (example in the Vollzugshilfe zur Störfallverordnung). In this way it can be prevented that because of stress important details are forgotten or are indicated too late. However, the extent must be designed in a way that the execution does not impede the operational procedure unnecessarily. The responsibilities have to be determined that the information flow is guaranteed.

Area **SMS: Planning for emergencies**

Question 6: How are the regulations towards the notification requirement evaluated?

Help:
There have to be written regulations in the establishment for conformance of the notification requirement according to German Major Accidents Ordinance.

For big companies this can be realized on the level of procedure/ process descriptions etc. or could be part of the emergency plan or a procedure/ process descriptions for external communication. For small companies this could be e.g. a part of the management manual.
The responsibilities of the involved employees and their authorities for the tasks in the framework of the notification requirements have to be regulated clearly and definitely.

There may be an interface to the internal reporting system (see area SMS: Monitoring performance, help to the question "How is the process "internal reporting system" or the regulations of registration and handling of incidents evaluated?"), because notifiable incidents can also be integrated there.

The regular review of the regulations has to be guaranteed. This can be realized e.g. in the audit system.

The operator has to notify an incident to the competent authority according to § 19 German Major Accidents Ordinance, if it meets the criteria for Annex VI part 1 German Major Accidents Ordinance. The operator has to submit immediately, at the latest 1 week after the incident, a written supplementary notification to the competent authority, which at least includes the information according to Annex VI part 2 German Major Accidents Ordinance. The operator must complement or correct the notification immediately if there is an existence of new knowledges.

For the operator of an establishment there may be other notification requirements e.g. according to the "Betriebssicherheitsverordnung" or according to the "Umwelt-Schadensanzeige-Verordnung" (environmental damage notification ordinance).

Area **SMS: Planning for emergencies**

Question 7: How are the regulations towards the crises management group evaluated?

Help:

Elements from the KAS-Leitfaden 29, Chapter 6.3 Notfallmanagement – Technische Einsatzleitung, Krisenstab (technical operations management, crisis management group):
Below there are described different aspects and specifics of the emergency planning on the basis of examples from big chemical companies.

For small and medium-sized businesses the corresponding requirements count as well and should be implemented appropriately. As best practice companies, which doesn't have corresponding resources, do cooperate with the corresponding external agency (e.g. competent authority, fire brigade, emergency management authority, etc.) and create a joint procedure for potential emergencies as defined by the points above (see also VCI-Leitfaden Notfallmanagement – Gefahrenabwehr 2010, Merkblätter Band 45: Musterkonzept für die Notfallplanung, LANUV NRW (emergency management - hazard control: sample concept for the emergency planning)).
Therefor organization units have to be built by the operator and the authority. Generally they are composed of an operational ("technical") operations management and an organizational unit (crises management group). These units are a special form of organization, which is not a permanently institution and are build and occupied dependent on incidents for a limited period according to a predetermined organization plan.

The **technical operations management** leads and takes the responsibility for measures of operational hazard control and must be made available by the plant or public fire brigade. It is responsible for the immediate measures on the spot and the communication to external crisis management units as well as to the crises management group.
Members of the technical operations management are managers of the internal crises management group, that means for example of the plant fire brigade and of the plant and process safety unit. In companies which doesn't have a plant fire brigade the leadership of the technical operations management is up to the competent authority for hazard control. In the cases of catastrophes this also counts for companies with an own plant fire brigade.

Independent of the plant fire brigade availability companies and competent authority should have a **crisis management group**.
The coordination of supporting measures for hazard control falls to the crises management groups. They take the responsibility for the internal and external communication and represent the company towards the public.
They are occupied by persons with key skills (see below) under the direction of a responsible person with managerial experiences that is able to make quick decisions under pressure.

Area **SMS: Planning for emergencies**

A typical crises management group is composed of plant manager, incident manager as well as persons from the functional areas communication and public relations, health, safety and environment. In addition a representation of the correlated area has to be consulted that can give information to the plant and the substances.
All these functions have to be hold available in a continuous 24/7 standby.
In no case the company management (e.g. Chief Executive Officer- CEO) should undertake the leadership of the crises management group. Their duty is to handle the different stakeholder interfaces (e.g. customers, the public).

The **authorities of a crises management group in case of an incident** have to be regulated in an agreement with the producing divisions:

- Right of access, “key-lordship” (for example performed by the plant security)
- Authorities for load changes/ shutdown of production lines
- The right to conduct reduction in the substances and energy network in case of incidents
- Authority to give directives towards members of other divisions or companies
- Permission to circulate information to the competent authority and the public, as possible coordinated with the hazard control

Typical duties of a crisis management group are:

- To establish a basis for operation (meeting, build a communication path to the technical operations management and other units, sum up the situation– state of incident combating, incident description, situation extrapolation)
- Informing (concerned population/ operation unit/concern, competent authority, police, public (press conference, press release) media information, citizen telephone)
- Identify hazard – warning (resolve participation of dangerous substances, immission measuring, sampling, warn the employees, warn the public (via operation centre))
- Support incident combating (support of the technical operations management, organize protective measures for the environment, arrange technical measures, (emergency) power supply, shut down plants, secure plant area, shut off the area, evacuate the buildings, shut down ventilation etc.)
- Aftercare (press conference, lessons learned session, arrange further measures: release/blockage of the plant area, extinguishing water disposal, investigation of reasons and amount of damage etc.)

The crises management group could and should obtain external support for following tasks if they are necessary and cannot be performed in the company:

- Psychological care for persons involved and concerned
- Call centre service for the public
- Data management
- Logistic
- Transport
- Accommodation
- Communication

Area **SMS: Planning for emergencies**

There has to be a room for the crises management group that is equipped with the appropriate technic for the crises management. Therefor there must be a reflection which technic, e.g. communication tool, should be designed redundantly and for which an emergency power supply has to be planed. It must be sure that the technic is checked regularly and if necessary is maintained. The use of technical tools should be trained.

Furthermore the following rules for the design of crises management groups should be observed.

Crises management groups act in seclusion, preferably in a non-public operation center, but not on-site. The crises management group is a consulting and coordination committee that in case of crises incurs the leadership of the emergency and crises organization as well as prepares and supports the decisions of functionaries. The interfaces to other organizations/units have to be planed. The crises management group has a clear structured and hierarchic organization form (similar to the military). Managers must be able to lead flexible in emergency situations, for example directive during a very dynamic situation, but in preparation and follow-up open and integrative.
The members of a crises management group should undertake functions that they have in normal operation but also must be willing to undertake other tasks. In the crises management group there should also be members that have experiences with competent authorities, press and the public.
Necessary are written functional descriptions with tasks, responsibilities, competences and interfaces. Important is that competitive double tasks have to be limited.

Members of crises management groups must have the following individual competences

- communication skills
- critical ability, cooperativeness and confidence
- decision-making ability
- problem-solving competence
- knowledge of resources and limits of her/his own person
- working under emotional pressure

and having the following skills

- information processing and integration
- definition of key activities
- structures and mechanisms of teamwork
- methods of decision making
- flexible modification to the circumstances , that means members of the crises management group must have deepened competences (see table 1 Leitfadens KAS-20 „Kompetenzen bezüglich menschlicher Faktoren im Rahmen der Anlagensicherheit“ (“Competences towards human factor in plant and process safety”)).

Area **SMS: Planning for emergencies**

Question 8: How is the cooperation with the off-site emergency response and emergency rescue service evaluated?

Help:
The cooperation of the unit that is commissioned with the operational hazard control (e. g. plant fire brigade) with external emergency and secure services (e. g. public fire brigade) should be defined clearly and regular reviews should be done. It is useful to do parts of the emergency exercises together with the public fire brigade. It is also possible to make an education and technical support of external emergency and secure services by the unit that is commissioned with the operational hazard control, so that in emergency there doesn't have to be a long instruction (e.g. description of entrance, special hazards etc.). It is pointed to § 12 German Major Accidents Ordinance where the operator of an upper-tier establishment has to instruct a person or unit with the limiting of major accident effects and to mention it to the competent authority.

Area **SMS: Planning for emergencies**

Question 9: How are the regulations towards the equipment of the operational emergency response evaluated?

Help:
There exist criteria to occupy staff for hazard control and its equipment, the responsibilities are determined. A regular review of the criteria has to be done. The staff for hazard control and the equipment should harmonize with the knowledge from the hazard analysis, so that it is clear how all potential accidents in the establishment can be dominated.
Furthermore the analysis of operations and emergency exercises as well as experiences of other hazard control units must be considered (regular exchange of experiences). There are regulations that ensure that the equipment of the unit commissioned with the operational hazard control at least correlate with the regulatory requirements. For the preparation of emergency cases the existing equipment and tools have to be checked critically. Because an emergency situation generally is stress for the participants, all aspects have to be limited that do need mental capacity, e.g. by a ergonomic design of displays (KAS-Leitfaden No. 29). More information and examples see KAS-Leitfaden No. 29.
If the hazard control members are strengthen by employees of the plants in the establishment it must be sure that hazards arise hereby on other places.
The personnel of a central notification unit could in particular cases function as a control centre if necessary, because all information converge there.
The responsibility for all mentioned points and the review cycles have to be determined.

Question 10: How is the procedure towards the equipment of the establishment with required warning devices evaluated?

Help:

There exist regulations which determine the necessary warning device as well as their implementation and evaluation. The responsible persons therefor must be defined. It has to be ensured that die necessary devices work in case if an incident (e.g. power supply).

Area **SMS: Monitoring Performance**

Area

SMS: Monitoring Performance

Question 1: How is the process of safety management system review according to aims and regulations evaluated?

Help:
The review of aims and regulations of the SMS follows a defined procedure and includes the review of the SMS aims and regulations. That means how successful the regulations are implemented in the SMS. The aims can be evaluated in management reviews and are described in the following area.

Usually the SMS review of the regulations in the establishment will be done in an audit system. The audit system of the Safety management system is a fundamental guidance element. It acts as an indicator for the implementation and efficiency of a safety management system.
The audits provide evidence of existing deficits and suggestions for their elimination.
The process of the audit system is discussed in the question "How is the process of the audit system evaluated?".

Small companies can realize the reviews in another way, e.g. in a definition of the review procedure as a part of the major-accident prevention policy (MAPP) or a review by using a checklist.
But an auditing by service provider is recommended also in a small company, then in periods of 5 years.

At the determination of the procedure and evaluation of the criteria e.g. in a chapter of the management manual the following aspects can be described:

- Dates for reviews and their principles, e.g.:
- Internal performance <name>, e.g. company owner by using the general checklist <name, date, reference> (this includes e.g. a list of all process, operating and work instructions) as well as special checklists<name, date, reference> e.g. for plant components <list>

and/or

- Procurement of audits to a service provider: in principle or by meeting certain requirements, e.g. every xx years, in a special technical sector or special plant components
    - Mention of criteria which have to be fulfilled by the service provider to guarantee a good quality of the audit. (e.g. qualification of the external auditors)
    - The contract design has to guarantee a (partial) independence of the auditors in regards to the results.

Area **SMS: Monitoring Performance**

- Contents of the review/audit documentation (e.g.: The annual review of the SMS regulations is documented by the storage of filled out general checklist “instructions in the establishment”.) and retention periods,
- Handling of review results
- A guarantee for the implementation of necessary measures detected from the review/audit results (e.g. Tools: to-do list with status display, filled out forms), who is responsible for it and how it is documented,
- Explanations, how the review procedure as well as the checklists are verified and how the being up-to-date is ensured

Further notes:
The checklists for dissimilar plants/task areas can be designed differently, the review periods as well.
The review results are part of the evaluation of the safety management system efficiency. These can be published internally. The publication of the results can animate the employees to archive improvement.
The used procedure of the review has to be evaluated regularly e.g. are the reviews sufficient towards periods or areas/plants etc.

Area **SMS: Monitoring Performance**

Question 2: How is the process of the audit system evaluated?

Help:

Main indicators of a (safety) management system are evaluation cycles that guarantee a continuous modification and improvement. The essential tool for the guarantee of evaluation cycles is the “Audit system”: the regular performance of audits by definite boundary conditions. In audits a process is evaluated (operations and their results) with regard to specified requirements (e.g. process instructions, norms and laws). An audit system is part of a verification that in the company a safety management system is established, works effectively and is suitable for reaching the determined aims set in the safety policy.

The process “audit system” has to be documented in writing in the form of a procedure/process description or management instruction. This documentation should include the following points:

- Aims, that should be reached by the process “audit system”
- Scope of application (e.g. establishment, organization unit of the establishment),
- Definition of terms
- Description of process steps and procedures in the context of the audit system (setting of audit plans, performance of internal and external audits, naming and qualification of the auditors, pursuing measures)
- Determination of the contents of process steps and tasks
- Determination of task authorities and responsibility
- Consideration of interfaces between separate processes (in particular implementation of subsequent measure/pursuing measures, management review)
- Handling of audit system results
- Regular audit review
- Determination of documentation contents (in the process steps)

The audit plans have to consider the points of the SMS reasonably (organization and personnel; Identification and evaluation of major hazards; operational control; management of change, Monitoring performance, audit and review)

In accordance to KAS-Leitfaden Nr. 19:
The types of audits differ, e.g.:

- *Internal audits:* auditors are employees of the company
- *External audits:* auditors are employees of an external organization
- *System audit:* It observes the operational and organizational structure and if all elements/aims of the SMS are considered
- *Compliance audit:* evaluation of the analogy to the approval notice/terms, technical regulations, works standard specifications, process instruction etc.

Area **SMS: Monitoring Performance**

- *Process audit:* evaluation of single processes e.g. hazard analysis, monitoring of the company, maintenance, management of change, announcement of major hazard accidents and near accidents, education and training arrangements, documentations)

Further notes to the process "audit system" (in dependence on: KAS-Leitfäden Nr.7 and 19):

- Determination of qualified lead auditors with authorities and responsibilities and experience in auditing. He/she represents the audit team at the top leadership of the company/site or rather head office/company management depending on the corporate structure
- Generation of Audit plans (internal/external audits)
  - units for auditing (e.g. departments, processes)
  - extend of audits
  - depth of audits
  - audit period (regular, occasion-related, incident-related)
  - working documents (checklists, forms for audit finding and conclusion/ recommended corrective measures)
  - involved persons (audit team)
- Naming of the auditors
  - qualification of the auditors
  - authorities of the auditors
  - guarantee for (partial) independence of the auditors
- Performance of audits
  - fix dates
  - involved persons (for the auditing areas)
  - signed documentation of the audit finding and conclusion
- Pursuing measures
  - initiation of corrective or preventive measures
  - agreement with the respective department
  - inclusion of measures in the to-do lists of the respective department
  - implementation of deficits/ corrective measures in the audit plan
  - subsequent audits
- Documentation/ reports
  - generation and presentation of the (annual) report that includes the results of conducted audits, presentation at the top leadership with the following aspects:
    - number of conducted audits
    - state of aim achievement of the audit plan
    - accumulated audit finding and conclusions (deficits/best practice)
    - continuative awareness and proposals
    - state of the pursuing measures
    - documentation inside of the audit system (interface to the navigation of documents)
    - responsibilities
    - retention periods

Area **SMS: Monitoring Performance**

- Regular reviews of the audit system (realized by reviews or external auditors: the audit intensity is followed by the number, extend and depth of conducted audits. This intensity has to be calculated that in consideration of establishment specific conditions the superior aim of the audit system is reached.):
  - Registration of all relevant units for the audit
  - Qualification of the auditors
  - Aptitude of checklists

There are definite criteria for the structure of an audit system. The following aspects can be concerned: the definition which areas are audited at which date; audit contents; concerned persons; the handling of audit results; audit documentation; regular evaluation if the conducted audits are sufficient (number, form of audit findings, audited areas). For all points the responsibilities have to be defined.

There have to be criteria for the determination of auditors. Criteria that can be relevant are e.g. qualification (education/further education (technical, psychosocial, organizational areas), experience), personal suitability, authorities. A (partial) independence of the auditors has to be guaranteed. The criteria as well as the acceptance and the implementation has to be evaluated regularly.

A definition exists for the criteria of the audit documentation (extend, contents: state description, agreements, signatures, responsible persons/ participant, dates, pursuing measures, retention periods, maintenance). The audit results can be documented in a checklist and summarized by the audit leader in an audit protocol and signed by the audited unit of organization. This ensures the protocol acknowledgement of the unit of organization. The audit protocol can directly be distributed to the audited unit of organization and the management of this unit.

It has to be defined how to handle the awareness of the audits and which consequences can be drawn. Stepwise regulations can exist therefor with regard to the authority for decisions, which measures have to be taken, responsibilities at the implementation of measures, periods for implementation, reporting commitment and publications. This concerns not only the deficits and defects but also the transfer of the best practice.

The responsibilities for all points above are defined.

If in an audit deviation or weak points are determined, these can be specified by the audit leader. Proposals to eliminate weak points can be part of the audit or a continuing procedure should be defined.
It makes sense to organize a trade off with the responsible auditors of the audited unit of organization to get conformity in regard to the audit results, e.g. regarding the evaluation of the found weak points., the conducted corrective measures, the for the conduction responsible persons and in compliance with the time frame.
If there is no agreement, this should be documented in the audit protocol. Determination how to manage this should exist as well.

Area **SMS: Monitoring Performance**

In case of a conflict with the concerned company at the execution of improvement measures there may be a conflict resolution model that informs the respectively superior or the executive council has to decide if necessary.

The responsibilities for the implementation of subsequent measures from the audits have to be defined. Appropriate competences and resources have to exist. This also counts for the definition of a time frame for the implementation of the measures.
The impact of the subsequent measure towards plant and process safety has to be checked (see area SMS: Management of change). The defined corrective measures should be evaluated regularly in regard to practice and effectiveness. The responsible persons for the control if the subsequent measures are implemented properly have to be determined.
This also counts for the consequences if measures could not be implemented properly. The competences of the responsible person have to accommodate therefor.
To the points above there should be an appropriate documentation.

Question 3: How is the procedure to eliminate deficits that had appeared in the emergency trainings evaluated?

Help:
There have to be criteria for the procedure to eliminate deficits that had appeared in the emergency exercise. The criteria could be e.g.: evaluation of deficits, definition of the period for deficit elimination, implementation of works for deficit elimination, review if measures to eliminate deficits are successful. There are regular reviews, if the defined procedure is observed and if the procedure and its criteria are effective. The responsibilities for all points above have to be determined.

Area **SMS: Monitoring Performance**

Question 4: How is the process "internal reporting system" or the regulations of registration and handling of incidents evaluated?

Help:
The registration and utilization of incidents such as accidental conditions, near misses, accidents and major accidents is part of learning lesson to handle incidents. This can be implemented in big and medium-sized companies in the form of a in-ternal reporting system, described in "Leitfaden KAS-8 Empfehlungen für interne Berichtssysteme als Teil des Sicherheitsmanagementsystems gemäß Anhang III Störfall-Verordnung"

In this guideline incidents are:

- Deviation of regulations
- Insecurity in acting
- Noticeable problems in engineering, organization or human factor
- Potential or latent critical situations
- Unusual conditions
- Every accidental condition of normal operation, that causes a release of matter
- Defects and deficits at protection system
- Immediate significant hazard of safety and health
- Notifiable incidents in terms of Annex VI, German Major Accidents Ordinance

The internal reporting system includes the procedure for incident registration and analysis, the deduction and implementation of measures as well as communication and transfer of the incident analysis in learning lessons.

The incident analysis has to be operated by a systematic (holistic) analysis method. Holistic means that the analysis method has to take care of all interaction of human, technique and organization (cp. MTO-Analysis). The knowledge of the incidents analysis is communicated internal as well as external in a document called "Learning Lessons" depending on e.g. transfer potentiality, risk potentiality and importance.

The process of the internal reporting system has to be documented in writing at the establishment e.g.in the form of process / procedure description/ management instruction etc. In this process the following points have to be included:

1. Aims which should be reached by the process
2. Scope of application
3. Definition of terms (e.g. incident, accident at work, major accidents notification, (holistic) incident analysis, Learning Lessons)
4. Description of process steps and procedures of the internal reporting system
5. Determination of the contents of process steps and tasks (systematic registration of notifications, selection of notifications that should be taken for the incident analysis, (analysis method, expertise, etc.) deduction and implementation of measures, publication of results from the incident analysis and internal/external trends of notifications)
6. Determination of task/process step authorities and responsibility

Area **SMS: Monitoring Performance**

7. Consideration of interfaces between separate processes (e.g. further education, hazard analysis, operational control, emergency planning, safety indicators, management review)
8. Determination of documentation contents at the process steps (i.a. appropriation of forms for notifications, review report of the incident analysis, abbreviated version (Learning Lessons))

Notes to the points above:
There have to be regular reviews if the defined contents of the process internal reporting system (criteria, procedure, responsibilities) are appropriate e.g. in the framework of audits.

Detailed information to organization, implementation and embedding of the internal reporting system into the SMS can be found in chapter 2.5 of "Leitfadens KAS-8 Empfehlungen für interne Berichtssysteme als Teil des Sicherheitsmanagementsystems gemäß Anhang III Störfall-Verordnung"

The points above count for big and medium-sized companies.

Prior condition for beneficial and good results at the process "internal reporting system" is a constructive error culture (see area SMS: Audit and review) and a positive developed notification culture.
It is important that the notification culture is implemented openly by the superior authority in example so that employees notify appropriate incidents: "what is not notified cannot be analyzed – what is not analyzed cannot be improved." /Leitfaden KAS-8/

Small companies have human resources of limited suitability to implement the process "internal reporting system" completely and to establish e.g. an own position for the internal reporting system.
Anyway, the learning from incidents is an important resource to identify and implement improvements in the company, financial benefit inclusive.
E.g.: The major hazard commissioner can receive the notifications of incidents, depersonalize and register them during the amplified analysis, regular system reviews and the communication of generalized results and suggestions ("Learning Lessons") is an external service.
The possibility to adopt parts/tasks of the process "internal reporting system" of several small companies can be eventually realized e.g. by associations etc.
The registration and handling of incidents in small companies has to be defined and documented e.g. in the MAPP, management manual, etc.
Documented aspects could be:

- Notification of incidents (definition) to a named person by employees, e.g. major accident commissioner.
- Implementation of round tables to issues such as Learning from incidents/ notification culture of company employees, e.g. twice a year
- Internal implementation of incident analysis: e.g. <name> e.g. company owner by using the method(s): ranked on the basis of the incident: <name, reference> (a possibility to analyze an accident occurrence is given by the Guide-

Area **SMS: Monitoring Performance**

line>„Ganzheitliche Unfallanalyse – Leitfaden zur Ermittlung grundlegender Ursachen von Arbeitsunfällen in kleinen und mittleren Unternehmen“ von B. Fahlbruch, I. Meyer (free pdf see Chapter references, further methods are described and evaluated there towards the SMB-suitability)

And/or

- Procurement of incident analysis to external service: principal or in case of special criteria e.g. incidents of …,
- Handling of the incident analysis results, internal and external communication inclusive.
- Guarantee that necessary measures that are generated from the incident analysis are implemented (e.g. tools: To-do-lists, filled out forms), who is responsible for it and how it is documented,
- Explanation which aspects of incident registration and handling (e.g. number of announcements, incident analysis, implemented measures, communication, contents of the round table) are included in a management review
- Regular reviews of the rules for incident registration and handling

Further explanations:
The registration of accidents and near misses has to be arranged systematically in definite criteria, e.g. definition of the notification requirements, how and to whom they are made, what has to be notified and documented. This can be realized in a stepwise concept. The investigation of the cause of an accident is regulated in a guideline or determination following definite criteria. Different aspects should be considered for possible cause areas such as material, technical, organizational, management specific, physical, psychical, social. A stepwise procedure can be realized for the investigation of the cause of an accident following aspects such as responsibility for implementation of investigation, persons which have to be consulted, internal investigations and external services.

The working atmosphere has to be created in a way that mistakes are handled responsible and open-minded to avoid that they are covered. Measures from the identification of cause of an accident have to be defined. The handling of the cause of accident and near misses results has to be regulated in fixed criteria. Affected are for example the implementation of measures in the establishment, the responsibility for the decision, which measures have to be implemented in which time, the internal and external publication of the investigation results.

The contents and compliance of the rules above are evaluated regularly. The evaluation also includes if the rules for the registration of accidents and near misses are appropriate to resister all relevant results. The handling of the evaluation results have to be defined.
The responsibilities for all points above have to be determined.

Area **SMS: Monitoring Performance**

Question 5: How are the regulations for using safety performance indicators in the plant and process safety evaluated?

Help:
To illustrate the proficiency level of processes of a company or organization in a short form, (efficiency) reference numbers or indicators can be identified. Reference numbers include in concentrated compact form information which is qualitative and quantitative ascertainable, by describing the circumstances and relationships mathematically and basing on measurable data/facts.

The process safety of establishments and their plants, the efficiency of the safety management system (SMS) inclusive, can be described by reference numbers or indicators.

Indicators can be divided into two types:
- an (negative) accident had already occurred:
Lagging indicators, reactive reference numbers or result indicators etc.
- an (negative) accident hadn't already occurred:
Leading indicators, proactive reference numbers or activity indicators etc.

For process safety the following indicators can be important:
Lagging indicators (absolute):
- Number of accidental releases (classified according to the amount and the substance characteristic hazardousness)*
- Number of fires
- Number of explosions
- Number of installation shutdowns or manual emergency shutdowns

Leading indicators (relative):
- Proportion of the done safety-related reviews
- Proportion of not in time (periodically) done hazard analysis
- Proportion of in time done measures of audit follow-ups

Further aspects of ascertainable indicators could for examples be qualification, instructions or the implementation of other safety-related organizational measures.

* e.g. according to the VCI-Guideline:
Loss of Primary Containment(LoPC) above the following qualifying quantity
- GHS Category acute toxic Cat. 1. and 2. as well as muta 1A, Carc. 1A, Repr. 1A, STOT SE 1 > 5 kg
- Any other classified substances according to GHS > 100 kg
- any other, not classified substances according to GHS > 2000 kg

Most of the time the terms indicator and reference number are used synonymic. It is also possible to differ indicators and reference numbers. Then indicators are substitutional parameters which correlate with relevant parameters and illustrate a parameter/ matter of fact by approximation (representation of "soft" factors). In this spirit indi-

cators are used in case of not direct measurable or not direct observable matter of facts.

At the **inspection** the following questions can be asked to the operator of an establishment:

- Are indicators for process safety/ plant safety set?
- For what reason are the indicators used by the operator?
- Which trends can be seen in the establishment?

For a better valuation of this thematic the inspector should have a look at the available documentation of the operator.

The registration of indicators for plant and process safety is used to enable a result-oriented regulation by the comparison of determined plant and process safety aims. Therefor an appropriate communication and participation of the top management is important. The regular ascertainment of indicators allows comparisons, e.g. over a period of time, between organization units (benchmarking) or target-performance comparison.
These questions may be answered:

- Are there changes compared with the previous year? What is the trend?
- How good are we in comparison with other companies or units or organizations?
- To what extend did we reached to our aims?

If there is a deviation from the aims the reasons have to be analyzed and ideas for improvement have to be found and implemented in concrete measures for the company or single organizational units.

Especially for big and middle sized companies a systematic process should be the basis of the setting, development, support and use of reference numbers.

See „Leitfaden zur Erfassung von Performance-Indikatoren für die Prozesssicherheit“ (Januar 2015) of the VCI.

The OECD guideline “Guidance on Developing Safety Performance Indicators” recommends a 7-step process for developing performance indicators:

1. Establish a performance-indicators-Team
2. Define the leading criteria
3. Define lagging indicators and relevant benchmarks
4. Define leading indicators and relevant benchmarks
5. Register data and report on the results
6. Take measures according to the results
7. Evaluate and improve the performance-indicator-system

This process is a closed loop, step (3) and (4) can be iterative until an appropriate combination of lagging and leading indicators is found.

Area **SMS: Monitoring Performance**

Further hints from the VCI guideline „Erfassung von Performance-Indikatoren für die Prozesssicherheit“ (Januar 2015) (extract, slightly modified/ shortened):

The safety performance of plants and techniques can be evaluated by the Key Performance Indikatoren (KPI). The KPIs also include the process safety incidents (PSI) that are implemented regularly in the companies. They can be used in each industry. The indicator PSI includes incidents with less or not any effects to the humans or environmental, but are characterized by an accidental release or that the first protective covering has lost its effect.

This guideline defines indicators for procedure and plant safety and especially determines a basis for a consistent report system for PSIs.
The guideline defines limitations and requirements for an effective internal incident reporting system as well as consistent criteria to classify incidents as Process Safety Incidents (PSIs). Methods for the developing and use of PSIs are explained.

The aim is to present a reporting system that provides global, regional and national data of the safety performance to enable the top management to recognize the real performances and trends and so to prevent, limit and correct anticipated and unwanted safety relevant process incidents.

This guideline deals mainly with the definition and registration of PSI for the proses safety performance. It is related to occurred incidents with effects such as e.g. fire, injuries with a stoppage of at least 1 day or an incidents with an accidental release above the defined (see above) release volume. The PSI is suited in case of comparable production sites for a benchmarking and a trend analysis and gives the possibility for the top management to make a conclusion and to promote a continuous improvement.

Indicators that in contrast are for prevention monitoring, show in what extend the company is prepared for incidents. This means e.g. near-misses or the number of inspections that have been done in time. They are not part of the guideline, although they are an important management tool.
It is the responsibility of the company to keep these indicators in mind to arrange for an effective process safety management.

The successful introduction of a PSI-reporting system for the evaluation of the safety performance in an company should include the following:

The reporting system is implemented from the level of top management to the level of every single employee.
The advantage of such a reporting system is communicated clearly to the responsible management up to the top management. A misuse of the PSIR has to be prevented.
An internal small factory of a company can have a much better PSI than the mean value of the whole company. This is not automatically the same as a bad safety performance of the small factory.

Area **SMS: Monitoring Performance**

The top management should be encouraged to communicate the PSI. That's why the notification of incidents should have no influence on the performance evaluation of the managers or the bonus system. Process safety incidents and work accidents are usually caused by human failure or organization deficits.

An open climate that encourages the management and employees to notify deviations can help to improve the system.

Area

SMS: Audit and Review

Question 1: How is the systematic review and evaluation procedure of the major-accident prevention policy (MAPP) evaluated?

Help:
There are definite regulations in writing how the systematic review and evaluation of the major-accident prevention policy (MAPP) has to be done. According to § 8 German Major Accidents Ordinance the operator has to review the MAPP and keep it up-to-date:

1. At least every 5 years after first preparation or modification
2. At modification according § 7 (3)(major accident relevant changes according to § 3 paragraph 5b BImschG) and
3. At an incident according Annex VI part 1

The MAPP has to include the operators overall aims and principles of action, the role and responsibility of management, as well as the commitment towards continuously improving the control of major-accident hazards, and ensuring a high level of protection. In line with the systematic review, the top management has to evaluate if these contents in the MAPP are still correct and appropriate or if there is a need of modification. If a modification is necessary the MAPP has to be revised.
Responsibilities within the appropriate competences of the MAPP review implementation have to be defined on the basis of criteria and the abidance by regulations.
The MAPP review has to be documented.

At **lower-tier establishments** or **small companies** this is generally done by the management of the establishment and the procedure of the MAPP review could be described in the MAPP itself.

- Responsible persons
- Dates or period
- Criteria for the review have to be mentioned (e.g. accident rate, audit and review results (interface to area SMS: Operational Control), implementation of measures, training results, satisfaction of the employees (e.g. from appraisal interview, surveys) and new knowledge)

For **upper-tier establishments** the MAPP can be part of safety report.
The MAPP review could be included in the regulations of the safety report and/or the management reviews.
The overall aims for plant and process safety and major accident precaution of the upper-tier establishment management can be found in the company and/or safety policy of the company management and thereby have to be reviewed and evaluated by the top management (see helps to the question of the area SMS: Major-accident prevention policy and structure of the SMS: "How are the rules for checking the aims

Area **SMS: Audit and Review**

in the plant and process safety policy evaluated?" as well as "How is the corporate Governance (CG) for the plant and process safety of establishments evaluated?").

Area **SMS: Audit and Review**

Question 2: How is the procedure of the systematic review and evaluation of the SMS (management review) evaluated?

Help:
There have to be definite criteria in the establishment, how the systematic review and evaluation of the safety management system (SMS) with regard to the effectiveness and appropriateness to prevent major accidents and limiting its effects is done. The concluding evaluation of the SMS review has to be done by the top management of the establishment. Usually this is implemented in the scope of regular (annual) management reviews.

According to § 8 German Major Accidents Ordinance the operator has to review the SMS in accordance to Annex III as well as its implementation and if necessary update it:

1. At least every 5 years after first preparation or modification
2. At modification according § 7 (3) (major accident relevant changes according to § 3 paragraph 5b BImschG) and
3. At an incident according Annex VI part 1

The following is relevant especially for concerns and big companies:

Common practice is an annual management reviews by the management.
This is an appropriate period to be able to reach the aims of a management system. A period of 5 years is not productive. In contrast for the regular review of the company's policy a period of 5 years is appropriate (see helps to the question of the area SMS: Major-accident prevention policy and structure of the SMS "How are the rules for checking the aims in the plant and process safety policy evaluated?").

In the inspection the documentation of the last two done management reviews can be perused and the questions from the KAS Leitfaden Nr. 19 mentioned below can be asked.

The Definition of a "management review" according KAS-Leitfaden Nr. 8:
The management review is a regular evaluation of the management system and the underlying company's policy of an organization by the top management.
Suitability, appropriateness, effectiveness and topicality of the management system, company aims and policy have to be evaluated.
The results of the management review include decisions and measures to improve the management system, providing resources and naming aims.

The following definition of a management review includes elements of the KAS-Leitfaden Nr. 19:

In accordance to the safety management system the management review evaluates the suitability, appropriateness, effectiveness and topicality of the safety manage-

ment system, the major-accident prevention policy (MAPP) and the safety or company's policy on the basis of plant and process safety.
In case of an integrated management system the suitability, appropriateness, effectiveness and topicality of a management system towards the seven points that have to be regulated in the SMS according to Annex III of the German Major Accidents Ordinance, the MAAP and the company's policy are evaluated towards issues of plant and process safety.

In addition the establishment or company aims in issues of plant and process safety have to be evaluated (see help to question "How are the rules for checking the aims in the plant and process safety policy evaluated?", area SMS: Major-accident prevention policy and structure of the SMS).
Towards the general aims of plant and process safety, the following questions should be answered in the management review:

- Have the mentioned aims in plant and process safety been reached?
- Are new aims in plant and process safety necessary?
- Was the SMS suitable to support these aims?
- Are there new requirements that have to be implemented by the SMS?
- Which improvements are possible?

The top management decides due to the results of the management review measures for the improvement of the SMS or the integrated management systems, providing resources and the naming of aims in issues of plant and process safety.

The procedure of the management review, including responsibilities as well as dates and requirements of the management review documentation, has to be determined in writing (management manual).
The following determinations should be defined:

- Dates for the implementation of the management review (periods, e.g. annual, every two years, after a major accident/incident),
- Responsibility/ evaluation by the top management
- The Documents, which are responsible for the implementation of a management review.
- Understandability/implementation of measures (who, at which time, Evaluation of implementation)
- Documentation of a management review (what, who)

The top management of the establishment takes the documentation to evaluate the SMS. Criteria for evaluation are e.g.

- Knowledge of the identification and evaluation of major accident hazards or internal report system (registration and investigation of major accidents, near misses and interruptions)
- Number of accidents
- Analysis of the performed audits (deviation, deficits, improvements, best practice)
- results of the evaluation of the SMS efficiency, e.g. in terms of indicators

Area **SMS: Audit and Review**

- Provided means
- Status of measure implementation
- Analysis of personnel measures (training, qualification, employee attitude survey)
- Results of reviews
- Abidance by the laws (amendment, status of the approval, exceedance, being within the testing period)
- New knowledge state-of-the-art of safety engineering (effects on the establishment)

It should also be evaluated, if the determined measures of previous reviews are successful.

The following documents could be the basis of a management review that means they could conduce to the evaluation by the top management:

- Reports of the major accident officer
- Major accidents/single great extend incidents
- Reports of the performed audits and their results
- Status of measure implementation (in process, done)
- Realized distinguished measures in issues of plant and process safety
- Chronological development of relevant indicators in issues of plant and process safety
- Indicators of the internal report system (see help to the question "How is the process internal reporting system or the regulations of registration and handling of incidents evaluated?", area SMS: Monitoring performance) e.g.:
  - Number of total announcements
  - Number of realized deepened analysis,
  - Number of information transfer (Learning Lessons)
  - Information on recommended measures eventually differentiated in technology, human, organization.
  - Possible further Information for the management review:
    - Special single incidents, specified reasons
    - Results of the system consideration and trend analysis

Note: "In companies with high risk potential the KAS sees the evaluation of personal and professional competences of employees of all hierarchy levels as an important element of the management reviews." (Annex 4, KAS-7 /10/)

Area **SMS: Audit and Review**

Question 3: How is the safety culture of the establishment valued?

Help:

Definition of "safety culture" from the KAS-Leitfaden Nr. 8 (equivalent also in KAS-Bericht Nr.7):
Safety culture can be seen as a part of a company or organization culture and reflects issues of safety in standard specifications, values, attitude and behaviour.

"Safety culture" means a safety related attitude in all hierarchy levels.
All company employees should appreciate their responsibility for safety issues and should be able to use this responsibility with skills, means and competences.
The safety culture includes two main components. The first affects the overall responsibility of the management to verbalization and consequent performance of the safety related company philosophy, creation of an organizational structure as well as appropriation of necessary human and technical resources. The second component includes the attitude and behaviour of the personnel in all hierarchic levels as well as the communication between them.
The continuous improvement processes part of a well-developed safety culture.
This results a continuous improvement of the safety level in correlation to the level of legal specifications.

The quality of the establishment safety culture can be characterized by the following aspects:
Time, means and resources for plant and process safety are given to the employees. The more this is followed self-evidently the higher is the benefit. This includes also that the superior, to the point of the top management, is persuaded of the plant and process safety relevance and also acts on it by example.

There is an interaction of safety management system (SMS) and safety culture: a well realized SMS can be seen as a proof for a positive safety culture. At a poor safety culture the SMS will have many deficits, but the implementation or improvement of a SMS can also improve the safety culture.

Specific aspects of the safety culture can be found in the corporate governance, safety policy, error and communication culture and resilience.
The external communication of the knowledge from the service experiences and incidents (see internal report system) can be an indicator for a positive developed safety culture / KAS Bericht Nr. 7/.
To evaluate the safety culture there is a classification in levels of maturity or development. E.g.:

- Step 1: Pathological
- Step 2: Reactive
- Step 3: Calculational
- Step 4: Proactive
- Step 5: Generative (see Hudson)

Area **SMS: Audit and Review**

Or:

Step 1: Emerging
Step 2: Managing
Step 3: Involving
Step 4: Cooperating
Step 5: Continuous improvement (see Keil Zentrum)

Or:

Phases in accordance to Bradly-curve:

Step 1: Instinct
Step 2: Control
Step 3: Comprehension
Step 4: Cooperation (presentation K. Weißenborn)

In dependence on the used model of safety culture there are many analytical instruments for evaluation. An essential classification is the implementation in the establishment by an external expert or as a self-evaluation.

For demonstration there are statements of safety culture self-evaluation (see UBA-Texte 22/08 Einfluss menschlicher Faktoren auf Unfälle in der verfahrenstechnischen Industrie) which can be answered with: wrong, barely wrong, partially right, barely right, right and not relevant:

- For me it is important to be prepared for unexpected incidents.
- It is easily possible to benefit from the know-how of former colleagues.
- My work gets appreciated.
- I am telling the superiors if they are wrong.
- In my department physical components are checked regularly towards safety by an nonpartisan.
- I know that routine can be dangerous.
- I take part in procedure revision, which I work for.
- If someone is acting imperilling, I intervene directly.
- In questions of safety my superiors are setting a good example.
- I pay attention to potential hazards for others.

The Phases of safety culture are built on each other:

That's why it is wise to definite the level of development/ maturity and to implement appropriate measures for the further development of safety culture.

Examples (see K. Weißenborn):

Phase "Instinct" i.a. with specifications in the way "abidance by the laws", "Safety plays only a little role for the employees", "safety responsibility is the job of the health and plant and process safety commissioner (only)"- the safety culture can be improved if the top management campaigns for safety and if managers indicate by measures and action that safety is of particular importance.

Area **SMS: Audit and Review**

Phase "Control" i.a. with specifications in the way "management indicates engagement for safety", "discipline and rules for safety are important and they are monitored and controlled", "Strong focus on trainings"- the safety culture can be improved by a implementation of an SMS, performance of incident and hazard analysis, a management seen as fair-minded (appropriate handling in case of mistakes).

Phase "Comprehension" i.a. with specifications in the way "individual knowledge an engagement of the employees in safety issues", "principles of safety are known and accepted", "take care of one's own", "there is a trained and experienced way of safety behaviour"- the safety culture can be improved by the focus on the teams and team training, business partner management, cooperative management style.

Phase "Cooperation" i.a. with specifications in the way "Helping others to participate", "contributing own input to safety", "take care of others", "being proud of the establishment" - the safety culture can be improved by measures of co-creativity encouragement, internalization of the principles general optimum is more important than single optimum, teams lead themselves.

To the aspect of creeping change:
Creeping changes are (very) slow and rather continuous changes in (very) small steps. These are often not realized consciously by the people and the chance is missed to work against the undesirable development in an early noncritical stage.
Examples of creeping changes towards plant and process safety are:

- The hazard analysis of the establishment is done in cooperation with an external service. Over the years the hazard analysis is more and more done by the external service on its own, with only little cooperation with the employees of the establishment (e.g. by reason of changes in tasks and/or task quantity of the employee). The effects of this creeping change can be serious: the know-how of the establishment gets lost and interface problems increase (relevant information do not reach the employees appropriately, measures are not or not completely taken/implemented etc.).
- The frequency of taking Nitrogen from the corresponding pressure tank decreases (several times to once a month). This implicates an increase of the presser in the tank. Together with other conditions it results in a bursting of the tank with significant damage (flying debris up to 150 m).

At a higher development level of the safety culture, the perception is increased by an extended attention and mindfulness for plant and process safety. Together with an early reaction undesirable developments by creeping change can rather be prevented.

Hints for inspectors:
The safety culture has to be created and lived by the establishment itself. The inspectors can give impulses how the establishment is seen by "strangers", how the external image is seen. This can be differing significantly from the "self-image" of the establishment employees. A discussion with the operator what is right and what is

Area **SMS: Audit and Review**

wrong leads to nothing. Inspectors should work towards the willingness of the operator to deal with the external image and to think about questions such as “Why am I seen like that? Are corrections of the safety culture necessary?” Etc.

This counts analogically for the following asked evaluations of communication and error culture and resilience.

Possible (introduction) questions to safety culture by the inspectors:

- How is the safety culture evaluated by the operator of the establishment? With which indicators/measures?
- Are models of safety culture/ analytical instruments known to evaluate the safety culture?
- Which measures of the operator that are taken/implemented/provided serve also as a boost for safety culture?
- Are risk assessments for mental stress performed at the workplace in the establishment?
  Can knowledge be deflected in safety culture evaluation?

Area **SMS: Audit and Review**

Question 4: How is the communication culture of the establishment valued?

Help:
At communication culture there is the focus on the content and method of internal comprehension in a (big) group of people. The communication culture is an important part of safety culture and it is very important for knowledge management and notification culture in the context of internal reporting system.
The communication of an establishment can be divided in internal communication, the communication between the employees, and external communication (see also area SMS: Planning for emergencies).

The internal communication includes the transfer of information as well as the dialog and exchange between the executive director, the single levels of management and their employees in the establishment and can be subdivided in formal an informal communication. The configuration of the formal internal communication is the task of superiors. In big companies it makes sense to see the internal communication as an own process.

According to Führmann and Schidbauer there is a three-step concept of internal communication:

- Analytical (includes: assignment of tasks, research and fact reflector, status analysis)
- Strategical (includes: aims, reference group, positioning, massages and subjects, concretion)
- Operative (includes: instruments, time management, budgeting, efficiency control)

The communication culture can be divided in established and occasion-related elements as well as the content-related elements information and dialog/exchange. Communication instruments are e.g. employee journal, suggestion box, regular meetings, employee meetings, appraisal interview, intranet, leaflet, poster, kick-off-meetings etc.

Compared to the informal internal communication the formal internal communication should guarantee equal information of all employees with the aim to involve these in the company events and to support the job completion.

The internal communication includes e.g.:

- transfer of necessary information
- mediation of internal values and aims
- clarification of internal contexts
- stabilization of the cooperation between operating areas
- assurance of employee motivation and commitment

A good communication culture includes effective information, an intensive exchange between superiors and the employees and working internal communication channels between the employees. A good communication culture is supported by a good or-

Area **SMS: Audit and Review**

ganization of internal communication but also needs positive personal communication behaviour of every single employee in the establishment. This can be supported by e.g. education.

Communication is more than the transfer of information. Important are three elements of communication: transfer, acceptance and confirmation.
A message is transferred - than check if the message is received and understood - than check if an adequate action is implemented.

A positive aspect is a transparent, open and clear communication.

It makes sense to involve the knowledge of the employees (e.g. suggestions for improvements) as well as a regular evaluation of leadership qualities of superiors by the employees. This should be done anonymous and should be the basis to recognize relevant potential for change and implement measures therefor.

A manageable, useful documentation is an important part of the communication culture.

The transfer of review and audit results, the evaluation of the major-accident prevention policy (MAPP) and of the safety management by the management contributes transparency to the employees.

Area **SMS: Audit and Review**

Question 5: How is the error culture of the establishment valued?

Help:
The error culture is the part of the safety culture which defines the handling with error in the company/establishment (of an organization). It determines how the single employee of all hierarchic levels of a company handles error. A constructive error culture can only be developed and lived permanently in an atmosphere of mutual confidence.

A (human) error means that the planed procedure of activities cannot lead to the wanted result and cannot be ascribed to a random and unexpected occurrence.
An error can only be identified as such afterwards.

The definition of "error" and "latent error" from the KAS-Leitfaden Nr. 8:
There is an error in the human-machine-system if the result of the task performance is extend the given or situational admitted deviation, that means if work quality is out of tolerance action. Latent errors are errors that were not realized previously to the unwanted occurrence and may be special/ temporal far away from the active error but are significant involved in the appearance of the trigger action.
Latent errors in complex system represent a significant safety treat due to its principal concealment.

At a constructive error culture the handling with errors is not affected by the localization of the culprit but by the optimized correction of errors as well as by the adequate cause clarification.
A cooperative behaviour of the employees on every hierarchical level and between the hierarchical levels is beneficial. The Superiors up to the top management appreciate their exemplary function and act on it. The employees get encouraged to notify occurred errors, assumed hazard, near misses etc. and see errors as a chance to improve learn and develop. It must be obvious that at wilful violations clearly adequate consequences are following.

The constructive error culture is affected of the awareness that errors are part of human action and faulty behaviour does not result from incompetence or from bad faith. If this general acceptance is given errors are seen as a chance to learn how to improve the behaviour.

Area **SMS: Audit and Review**

Question 6: How is the resilience of the establishment valued?

Help:

Definition of Resilience (see presentation of Dr. Babette Fahlbuch):
Resilience is the ability of a (organizational) system (establishment) to anticipate risks and to handle them effective. Therefore it conforms its action, subsystems and processes in a way that its central function can be implemented solid and effective in the existing environment.
This property gets very important if the environment is not solid and this instability can lead to the destruction of the system (establishment).
Resilient organizations reach their company aims simultaneously and flexibly. Resilience is also the ability to return to normal operating after an accident/ a crisis. Resilience is a dynamic process.

Characteristics of a resilient organization:

- assertiveness: fast and effective reaction towards realized hazards (indicators: measure pursuit / To-do-lists of audit results/ emergency training etc.: contemporary implementation?)
- conservative decisions in safety issues
- flexibility
- resources
- to hold up the perception of (possible) hazards (before feeling safe because of routine)

Definition of Resilience (see presentation of Prof. Dr. Toni Wäfler):
Resilience is an extended view on safety, an enhancement of the SMS. The human is seen in this view (see Safety II, Hollnagel) as a safety factor and is the resonance adaptability (resilience).
The resilience contains in particular the ability of the organization to hold up the control under dynamic conditions. Resilience means the ability of an organization

- to adapt to changing imperilling influences efficiently (and not to avoid or resist imperilling influences) and
- to reach a dynamic and solid state, also and especially after incidents.

Premise in this case is:

  - Insecure states occur by insufficient adjustment and not by an error.
  - Safety occurs by proactive adaptive processes and not by reactive barriers.

The former view (see Safety I, Hollnagel) sees the human as the risk factor: human error occurs; the source of error has to be found and be eliminated by the guarantee of approved implementation.

Area **SMS: Audit and Review**

If under this view an incident analysis is performed it leads often to a hindsight bias: A back sight simplification and overestimation of incidents predictability.
Afterwards, routine actions are seen as errors if they had negative consequences. There are many reasons for deviation of regulations:

- too many regulations,
- regulations are not known or understood,
- discrepancies between the regulations,
- regulations are not practical for non-standard situations,
- the need to adjust the situation.

At researches of resilience there is no focus on errors (what went wrong), there is an analysis how success is reached (why things go right).

According to Hollnagel these is the **Efficiency-Thoroughness Trade-Off (ETTO)** Principle:
Humans and organization have to find a balance between (Action) Efficiency and thoroughness.

The principle ETTO is not the same as productivity and/or safety. It leads to variability in workmanship:

- The variability is a strength of humans because it allows him/her to assimilate.
- This variability can also contribute negative incidents. Than it is called “error”.

At standardization there are three types:

a. **Action specification** (detailed regulation for one concrete operative action procedure)
b. **Process specification** (guidelines/ checklists for the procedure)
c. **Aim specification** (Specification of the aim without a statement how to reach these aims

From a) to c) the scope of action and the effectiveness increases, but at the same time the insecurity rises.
To compare Safety I and Safety II a company (establishment) can handle areas with a small spectrum of deviation and errors or a good predictability of deviation and errors with stability, that means standards (clear Action specification, e.g. work instructions). On the contrary areas with a great spectrum of deviation and errors or a bad predictability of deviation and errors can be handled with flexibility/ adjustment, e.g. have to be managed by the orientation to aim specification.

At the configuration of regulations in the establishment it is important to consider the aspects above. This can be realized if the document structure has a central theme or a process orientation as it is shown in the help of the question „How is the documentation of the SMS in the establishment evaluated?“, area SMS: Major-accident prevention policy and structure of the SMS.
Generally there also has to be an adequate level of maturity/ phase of safety culture.

Area **SMS: Audit and Review**

In the scope of the inspections interviews with the employees of different hierarchic levels can be done to estimate the resilience. Therefore the following questions can be helpful:

- Were there any unexpected and/or critical situations that you have managed well?
- Which factors did help you to manage them successfully?
- Which hazards can be identified in your own task/ in the establishment?
- Are there any action specifications how to manage hazards? (Are deviations possible?)