Risk management

**1. Subject**

**1.1 Purpose**

**1.2 Scope**

**1.3 Glossary**

**2. Responsibility**

**3. Documents**

**4. Requirements of standards:**

* **ISO 31000: 2018**
* **ISO 27001: 2022**

**5. Development**

**5.1 Planning**

**5.1.1 General**

**5.1.2 Resources**

**5.1.3 Internal communication**

**5.1.4 External communication**

**5.2 Context**

**5.3 Identification**

**5.4 Analysis**

**5.5 Evaluation**

**5.6 Treatment**

**5.7 Monitoring**

History

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| All | Creation | 01/01/2024 |
| **Page** | **Change** | **Date** |

**1. Subject**

**1.1 Purpose**

The purpose of this procedure is to define the rules for identifying, analyzing, evaluating and reducing risks. The objective is to increase the overall performance of the organization by focusing on its core business and not on emergency situations.

**1.2 Scope**

We do not forget that zero risk does not exist and that any activity includes risks linked to:

* information security
* process security
* customer satisfaction
* document control
* data analysis
* staff competence (inadequate training)
* the deterioration of the image of the organization

External and internal issues relevant to the BCMS and actions to address identified risks and opportunities for improvement found are taken into account.

**1.3 Glossary**

BCMS – business continuity management system

Risk - likelihood of occurrence of a threat or an opportunity

FMEA - Failure Mode and Effects Analysis

**2. Responsibility**

Top management is responsible for ensuring the strict application of this procedure in accordance with the organization's risk management policy. All project managers, as risk owners, are responsible for managing the risks of their product or process. Each department of the organization contributes to the treatment (reduction) of identified risks.

**3. Documents**

**3 Documents**

Incident register

Risk register

List of risks

Risk treatment plan

Objective achievement plan

**4. Requirements of the standards**

**4.1 ISO 3100 version 2018 requirements**

6.4 Risk assessment

6.4.1 General

6.4.2 Risk identification

6.4.3 Risk analysis

6.4.4 Risk evaluation

6.5 Risk treatment

6.5.1 General

6.5.2 Selection of risk treatment options

6.5.3 Preparing and implementing risk treatment plans

**4.2 ISO 27001 version 2022 requirements**

6.1 Actions to address risks and opportunities

6.2 Objectives

8.1 Planning and control

8.2 Risk assessment

8.3 Risk treatment

**5. Development**

**5.1 Planning**

**5.1.1 General**

Top management involvement is an essential condition for the success of the risk management project.

Based on existing information and documents, project planning is started. The risk management process is part of the organization's overall management system and is adapted to our specificities.

Annual objectives for identification, analysis, evaluation and treatment of risks are set. Responsible people, roles and deadlines are established, recorded and communicated (see Risk Treatment Plan).

An assessment of the compliance of our organization's processes with applicable legal requirements is carried out by the information security manager.

**5.1.2 Resources**

Top management plans and ensures the necessary resources at each stage of risk management activities.

The training, knowledge, competence and experience of staff are critical.

Resources include the methods, process, documentation and equipment used.

**5.1.3 Internal communication**

Internal communication and consultation of information on risk management activities is recorded in internal reports.

The reports help staff understand the assessment and treatment of risks.

For each risk identified as unacceptable, a control measure is chosen (see Objective Achievement Plan).

**5.1.4 External communication**

External communication and consultation of information on risk management activities is recorded in external reports with the active participation of stakeholders (feedback, consultation, emergency plan).

**5.2 Context**

To establish the external context, first and foremost, we take into account meeting the requirements of external stakeholders.

To establish the internal context we mainly take into account the strategy and our corporate culture, the policy, the risk management objectives, the competence and perceptions of the staff.

The necessary resources are established and ensured (see paragraph 5.1.2).

The activities of the “manage risks” process are determined (see paragraphs 5.3 to 5.7).

The risk criteria are determined:

* types of causes
* types of consequences
* measurement method
* likelihood (probability) of the effects appearing
* acceptable level of risk
* combination of several risks

**5.3 Identification**

The list of all identified risks (potential and actual) is recorded and updated at least twice a year (see the List of risks file).

The active participation of all is essential because it is the personnel in the field who are best aware of real and potentially dangerous situations.

This list is the result of the work of the multidisciplinary team having reviewed the sources, causes, impacts, effects and consequences of the risks that may appear in our organization.

**5.4 Analysis**

Determining the causes and consequences of risks allows us to gather the data necessary to assess risks (see paragraph 5.5) and make risk treatment decisions (see paragraph 5.6).

One risk analysis method used is FMEA – failure mode and effects analysis. This analysis allows us to identify and evaluate potential failures and reduce associated risks with appropriate actions. FMEA is used by the information security department to analyze risks at different levels of the organization.

We use the following table to determine the likelihood of a risk occurring:

|  |  |  |
| --- | --- | --- |
| Likelihood of occurrence (O) | | |
|  | Detection | Frequency |
| 1 | Improbable | Never occurred |
| 2 | Very low | Once a year |
| 3 | Weak | Several times a year |
| 4 | Probable | Once a month |
| 5 | High | Once a week |

We use the following table to determine the severity of risk impacts:

|  |  |  |
| --- | --- | --- |
| Severity of impacts (I) | | |
|  | **Level** | Impact |
| 1 | **Minimal** | Negligible |
| 2 | **Minor** | Weak |
| 3 | **Moderate** | Moderate |
| 4 | **Major** | High |
| 5 | **Severe** | Critical |

Each risk is quantified in terms of its likelihood of occurrence (O) and the severity of the impacts (I) that it can have. The risk level (RL) is the result of multiplying the occurrence by the impact:

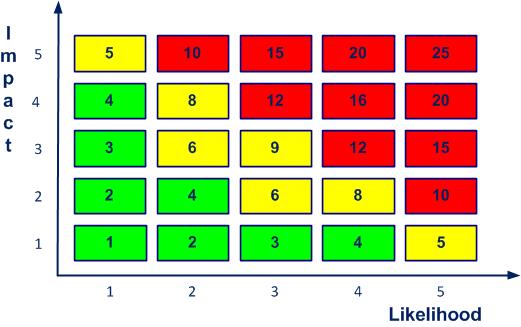
RL = O x I

In certain cases we can add factors such as the time of exposure to the hazard (multiplied risk) and the difficulty of detecting the risk.

**5.5 Evaluation**

We classify risks according to their level into three categories (see risk level figure):

* acceptable (1 ÷ 4) - green
* unacceptable (5 ÷ 9) - yellow
* intolerable (10 ÷ 25) – red



*Figure Risk level*

This allows us to make decisions on the priority and implementation of control measures to address risks (see paragraph 5.6).

The financial consequences play an important role in the assessment of risks and the decision to implement actions.

Risk assessment allows us to determine when a risk is acceptable and can be tolerated by the risk owner (level 1 to 4). Depending on the importance of the risk, the existing means of control remain unchanged.

For an unacceptable level of risk (level 5 to 9) we seek balanced control opportunities with reasonable and realistic costs (benefit/risk ratio).

When the level of risk is intolerable (level greater than 10) treatment of the risk is essential, whatever its cost.

Control measures to address unacceptable and intolerable risks comply with applicable legal requirements to which our organization has subscribed.

The risk assessment is based on:

* data review
* the benefit/risk ratio
* participation of stakeholders
* taking into account the worst case (extreme limits)

**5.6 Treatment**

When potential or actual risks are unacceptable or intolerable they are reduced, avoided or transferred.

The priority of actions is carried out on the risks with the highest level.

When the source of the risk is identified our efforts are directed towards eliminating the source.

Risk treatment is assessed by checking whether residual risks are tolerable and reviewing the effectiveness of control measures.

A comparison is made of the financial impact of implementing and not implementing each control measure. After this cost analysis, control measures are selected and responsibilities are assigned.

Risk treatment actions are regular and are described in the treatment plans. Each plan is recorded, dated, verified and validated by the person designated by top management (see job descriptions).

A combination of several risk treatment options is often used.

Communication and consultation with stakeholders, when choosing risk treatment options, is a guarantee that a new risk will not be created following the treatment of the old risk.

**5.7 Monitoring**

The aim is to verify the relevance of the analysis, the effectiveness of the control means put in place and the level of residual risks.

The people responsible for risks (see job descriptions) regularly carry out monitoring.

Feedback (incidents, complaints, results of corrective actions) is the database for driving continual improvement, cf. the Incident Register.

Monitoring records are kept in reports and are an input to the management review.

The data obtained after the sale of the products allows us:

* identify new risks such as unintended use
* update the analysis, evaluation and treatment of risks
* update the benefit/risk ratio
* improve the risk management process