SISTEMUL MEDICAL MedLife

MEDLIFE GROUP
Risk management policy
ERM guide

Table of Contents

RISK MANAGEMENT POLICY

Purpose

The purpose of this Risk Management Policy is to establish a structured and consistent approach to identifying, assessing, managing, monitoring, and reporting risks that may impact the achievement of the organization's strategic objectives, operations, assets, reputation, or compliance obligations. This policy ensures that risk management is an integral part of all decision-making processes within the organization.

Scope and Applicability

This Policy applies to all activities carried out by the legal entities of the MedLife Group (hereinafter referred to as "the Group"), as presented in the consolidated financial statements, as well as to any other legal entity that becomes part of the Group in the future. The Policy can be made available to employees, non-salaried personnel, patients and clients, and all relevant external stakeholders, including contractors and service providers, to ensure transparency and alignment throughout the implementation process. It covers all types of risks, including but not limited to: strategic, operational and financial risks (including sustainability risks included under any of the headings before).

Regulatory and Standards Alignment

Risk management is an essential component of good governance. The **global risk management (Enterprise Risk Management - ERM)** aims to preserve and continuously improve the value, reputation, and internal motivation of the Group. It encourages a reasonable level of risk-taking, acceptable to stakeholders and economically bearable. Achieving this goal relies on a good understanding of our risks and the skills to manage them. This Policy has been developed in consideration of the governance and compliance standards applicable at the time of drafting, including but not limited to:

- ISO 31000
- COSO ERM Framework

The Policy shall be applied in accordance with all relevant national and European legislation and regulations applicable to the Group's operations and its subsidiaries.

Governance and Responsibilities

This Policy was developed under the coordination of the Financial Department within MedLife S.A. and has been formally approved by the Chief Executive Officer of the company.

Within the MedLife Group, the Financial Division supports line management in the implementation, monitoring, and continuous improvement of the Risk Management Policy. It ensures that all risks — including environmental, social, and governance (ESG) risks — are identified, assessed, and integrated into the broader risk management framework of the Group.

Objectives

The objectives of this policy are to:

- Promote a proactive risk management culture.
- Minimize the likelihood and impact of potential threats.
- Enhance decision-making through informed risk analysis.
- Ensure compliance with applicable laws, regulations, and standards.
- Protect stakeholders' interests and the organization's reputation.

Training and Awareness

The organization will provide periodic training sessions to ensure all relevant staff understand the importance of risk management and are familiar with the processes and tools used.

Policy Review

This policy shall be reviewed whenever significant organizational or external changes occur to ensure continued relevance and effectiveness. All revisions must be approved by the Board of Directors.

CHAPTER 1: ORGANIZATION OF THE ERM GOVERNANCE

The CRO reports directly to the Board of Directors as provided by the BVB Code of Governance.

Contact / member of the ERM network	Operational responsibilities	Actions	Deliverables
Chief Risk Manager (HQ)	Responsible for the ERM exercise	• Prepare and lead the annual assessment • Be consulted on risk identification and assessment by entities • Challenge the risk reviews of entities • Coordinate with the various HQ departments • Develop and maintain the risk management framework and methodology. • Facilitate risk assessments and ensure consistent application of the policy. • Provide risk training and awareness programs	Final Group risk review
Board of Directors (HQ)	Approves the Risk management policy Define risk appetite Approves the annual risk review	• Validates annual risk review • Adjusts risk appetite and tolerance levels • Review major risk exposures and mitigation plans periodically	
Functional Departments (HQ)	Define risk assessment templates Support for action plans	• Identify risks • Define guidelines for risk assessments by their departments • Provide a 'second eye' • Implement measures and control actions • Contribute to the preparation of the Group risk review	Guidelines for risk assessment
CFO (HQ)	Owner of risks and mitigation actions	• Be informed of the risk synthesis and the implementation of global risk management	

It should be emphasized that the **Group's Board of Directors** are responsible for validating the final risk review presented by the CRO and pre-validated by the Executive Committee.

The CRO has a duty to "say what the risks are" and oversees the development of risk management skills and maturity within the Group.

CHAPTER 2: RISK MANAGEMENT METHODOLOGY

This chapter describes the risk management approach:

- Consider the context
- Assess the risk:
  - ✓ Identification
  - ✓ Analysis of causes and consequences
  - ✓ Evaluation based on scenarios
- Establish the target risk
- Set mitigation strategy and action plans
- Monitor and review risks

2.1 Consider the context

The first step in risk management is to understand the entity's activities, the environment in which it operates, and the internal/external elements or events that could jeopardize it.

To do this, the CRO gathers various types of information:

- within the Group: review of past events, analysis of strategic, financial and operational objectives, identification of stakeholders, etc.,
- outside the Group: analysis of industry trends, benchmarking against similar companies, etc.

2.2 Assess the risk

2.2.a. Identification

The CRO must have a thorough understanding of the issues facing the Entity (or Entities) and/or the country (or countries) within its (their) perimeter. The following actions will help to gather different sources of information to identify / discern the most threatening risks for the Entity:

- conduct regular (at least annually) interviews with members of his/her entity's Management Committee or Executive Committee, either individually or through ad hoc committees, and with other operational managers
- interact with the various managers of functional line within the entity.
- work with a multidisciplinary team at different levels of the Entity, in order to carry out an analysis of emerging risks or risks linked to new activities,
- use the *Risk Catalogue* as a working basis for risk identification, listing most of the categories of risk encountered in the Group's activities, although it is by no means exhaustive. In particular, the catalogue can be used to check that certain general risks have been considered in the review.

2.2.b Causes and consequences analysis

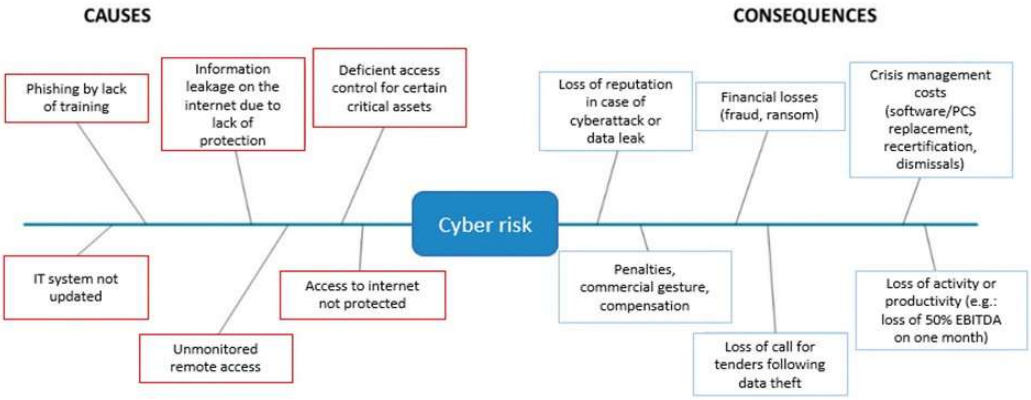
The occurrence of risk is generated by one or more causes and leads to one or more consequences.

Causes can be direct (directly triggering the occurrence of the risk) or indirect (promoting the occurrence of the risk, upstream in the causal chain, and/or reinforcing the extent of its consequences).

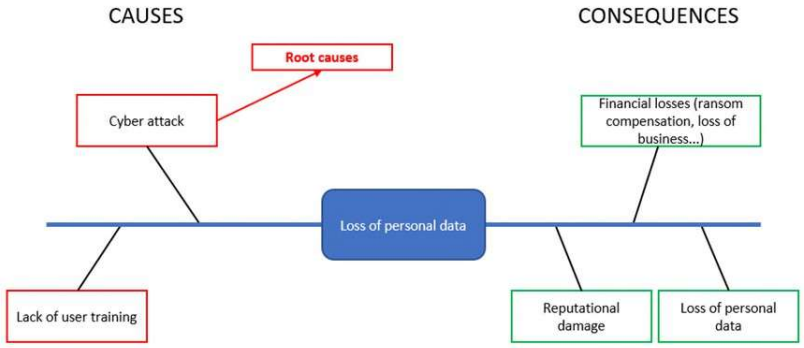
Several methodologies are available for carrying out this analysis and identifying causes (Ishikawa diagram or cause tree, 5 whys, etc.): MedLife uses the cause tree as standard, which is suitable for the simplest analyses. It is important to look for the root causes to increase mitigation effectiveness.

Consequences will generate impacts on the company. It is crucial to identify them correctly: failing to act on the causes, which are sometimes external, action on the consequences can limit the impact to acceptable or negligible proportions for the company.

Example 1: Example of an Ishikawa diagram showing Cyber risks



In the case of correlated risks, the consequence of one risk may also be the cause of another. Whether an event is a cause or a consequence depends on the point of view from which it is viewed. In the example below, the apparent cause of the loss of personal data was a cyber-attack: we need to go back up the cause tree to find the root causes, which could be, for example, a failure of the security or access control systems.



Example 2: Example of an Ishikawa diagram showing the risk of non-compliance with data protection laws

2.2. Evaluation of risk based on scenarios

Once the risks have been identified, along with their causes and consequences, they need to be assessed from two angles:

- **impact** and
- **likelihood**,

  using a scenario (i.e. a set of assumptions about the occurrence of the risk and its consequences).

An inherent risk is the materialization of a hazard: in an uncontrolled environment, its parameters (likelihood and impact) depend solely on the nature of the hazard and the environment in which the event occurs.

- **Inherent (or gross) risk which generally has high parameters.** Continuous actions (technical, organizational, insurance, etc.) are taken to reduce these parameters.
- **Residual (or net) risk:** The level of parameters resulting from these measures is that of the residual risk: it is this level of residual risk that is the subject of the global risk management system.
- **Target risk:** For each risk identified, the CRO determines a target risk level stating the exposure or risk-taking that he/she accepts, in compliance with the law and the risk appetite defined by the Group. It is characterized by a target level of impact and likelihood or defined by financial or non-financial indicators.

Risk scenarios

A risk is assessed on the basis of a **standard scenario**, the description of which makes it possible to define hypotheses for quantifying the impact and likelihood of the risk and to obtain consistency between these parameters. This assessment is based on 2 aspects:

- **Inherent** risk: before implementing mitigation plans, or in cases where ongoing actions are already in place, considering that these are ineffective
- **Residual** risk: after implementation of mitigation plans comprising ongoing actions and specific action plans

While the description of the risk may be general, the scenario must be detailed and consider the specific features of the risk (local context, project/asset concerned, assumptions of materialization, etc.) for an appropriate assessment.

Although risk assessments must be representative, they do not need to be very precise. Orders of magnitude are sufficient to determine whether the risk is potentially catastrophic or, on the contrary, minimal.

The **time** (or occurrence) **horizon** of the risk corresponds to the period over which the risk is likely to occur. It is closely linked to the scenario selected.

- **Short term:** the risk occurs within 1-3 years,
- **Medium term:** the risk occurs within 4 to 6 years,
- **Long term:** the risk occurs beyond 6 years.

Defining an **extreme scenario** can help to challenge the resilience of the Group's strategic orientations and investment decisions, and enables to estimate the degree of preparedness in relation to certain rare risks, in terms of both prevention and mitigation. The extreme scenario is based on reference accidents or events that are considered rare but not impossible.

Financial and non-financial impact

The **financial impact** is the cost for the Entity over the period of the scenario. It is assessed on a 4-level scale, from 1 for the lowest to 4 for the most catastrophic impact. By convention, it is compared to a reference quantity, which is generally the cumulative EBITDA over the Groups timeframe (Medium Term Plan).

Score	Impact level	Value range (% of reference quantity, EBITDA cumulated on 3 years horizon)
1	Insignificant	< 1%
2	Minor	Between 1% and 3%
3	Moderate	Between 3% and 5%
4	Major	Between 5% and 15%
5	Catastrophic	>= 15%

The financial impact of the inherent risk is expressed / assessed as the value on top / deviation from the budgeted base case scenario.

All the impacts will be examined, specifying their nature (EBITDA, below EBITDA, assets value, CAPEX, etc.).

For a clear understanding of the assessment of residual risk and its evolution, it will be necessary:

- to formalize the main underlying assumptions incorporated into the baseline budget and the modelling for subsequent years;
- to indicate the portion included in "provisions" in the budget.

Example of impact calculation: Cyber risk: A total of 151 MEUR for inherent risk, broken down into:

- *Cost of crisis management: 84 MEUR*
- *Loss of revenue: 40 MEUR*
- *Destruction of assets (workstations): 2MEUR*
- *Commercial indemnities: 25 MEUR*

Insurance covers part of the cost of crisis management, loss of income and asset destruction. The financial impact of the residual risk is reduced to 85 MEUR.

Non-financial impact

The non-financial impact is the measurement of the consequences for the Group (and where applicable for stakeholders) of non-financial aspects such as:

- human resources,
- the Group's reputation or image,
- environment,
- legal,
- social or societal,
- health and safety.

The non-financial impact is assessed on a 5-level scale, from 1 for the lowest to 5 for the most catastrophic impact.

Score	Impact level	Description (*at least one of the criteria below may result*)
1	Very Low	No or no serious impact on human health (*accident at work followed by modified postings/medical treatment/moderate effect on health*) or on the environment (*minor pollution with short-term impact (up to 3 months)*). Situation can be resolved in the short term. Local or low-level media coverage. Civil/commercial actions with limited financial and/or reputational impact.
2	Low	Some impact on human health (*serious or severe injuries: Lost-Time Accident (LTA) /without significant effect on health*) or on the environment (*minor pollution with a localized medium-term impact (up to one year)*). Real threat to the stability of the structure. Local or regional or limited national media coverage. Civil/commercial legal action with limited financial and/or reputational impact.
3	Moderate	Long-lasting or irreversible impact on human health (*serious or severe injuries: Lost-Time Accident (LTA) /significant effect on health*) or on the environment (*moderate pollution with a localized medium-term impact (up to one year)*). Real threat to the stability of the structure. Regional or national media coverage. Civil/commercial legal action with high financial and/or reputational impact.
4	Severe	High impact on human health and life (one death, serious injury/health effects/long-term disability) or the environment (serious pollution with localized impact lasting up to 2 years. Significant sanitization costs) Continuity of the structure jeopardized. Broad media coverage. Possibility of legal action against company officers.
5	Catastrophic	High impact on human health and life (*several deaths due to the same event*) or on the environment (*major pollution with long-term modification of the environment, irreversible damage*). Continuity of the structure severely compromised. Major media coverage and sustained adverse press campaign. Legal action against company BoD or Executives

Likelihood

In the absence of statistics or specific Group rules, the likelihood can be estimated by a combination of factors: the events that have taken place, the effectiveness of the mitigation measures in place (assessed using indicators), common sense, experience, etc. It is recommended that several points of view and several sources of data be combined. Explaining the factors that led to this estimate will make it easier to understand.

The likelihood of occurrence is assessed on a 4-level scale, from 1 for the lowest to 4 for the highest likelihood range:

Score	Likelihood level	Value range	Comment on significance
1	Rare	< 5%	There is a very low, but non-negligible possibility that the risk may occur.
2	Unlikely	5% - 25 %	There is a possibility that the risk may occur.
3	Possible	15%-25%	There is a moderate possibility that the risk may occur.
3	Likely	25 and 50 %	There is a clear possibility the risk may occur which is lower than the risk not occurring.
4	Certain	>= 50 %	It is more likely that the risk will occur, higher than the risk not occurring.

When the likelihood of a risk exceeds 50%, it is advisable to consider incorporating all or part of its impact into the budget/forecasts.

Recurring risk events are risks that have a chance of occurring every year with the same likelihood and impact. These are specific events which we know will probably occur, without knowing how many times over the budgeting horizon. By default, such risk to be assessed in the 1st year of the budgeting period (example: credit risk, risk of unavailability of some assets, cyber security risk, HR risk, etc.)

2.3 Establish target risk mitigation strategy and action plans

Risk appetite is defined as the type and level of risk that the Group is prepared to accept as part of its strategy to create value.

It is expressed in terms of acceptable variations or targets for indicators:

- **financial values** such as capital employed, EBITDA,
- **non-financial** values such as reputation with stakeholders,
- non-financial **indicators**: availability rate, satisfaction rate, accident rate, etc.,
- **exposure** limits or **attention thresholds** relating to the criteria defined (e.g. maximum amount of capital employed per country, volumes not covered in the case of market risks, insurance excess, etc.).

These criteria and limits are defined in specific risk policies, which also states risk management in certain areas, the procedures for dealing with risk and monitoring indicators.

Risk appetite may change over time as the Group's environment and objectives evolve.

2.4 Risk mitigation strategy and action plans

For each risk, an **owner** is appointed by management: this person is responsible for defining the risk management strategy and developing and implementing action plans designed to achieve the target risk level.

Action plans should target the causes of the risk, to reduce its **likelihood**, or the **consequences** of the risk, to reduce its **impact**.

The mitigation strategy is the global approach adopted to deal with the risk. It can be very varied. It will be all the more effective if it has been consciously chosen, constructed and adapted to the context of the Entity and the risk, rather than being the result of a sum of variously coordinated initiatives.

- **Remove the risk.** Cessation of the business, assets or relations with a stakeholder.
- **Reduce the risk** by:

✓ **Diversifying risk**: Spread the risk over several a priori independent activities or areas to eliminate the concentration effect. For example, diversifying the Group's geographical presence to reduce country risk. It should be noted that diversification has a powerful effect, but can fail for dependent risks, particularly in the case of systemic risk.

✓ **Implement control measures** (prevention, protection, development of internal control), prior and subsequent processing, etc. For example, implement segregation of duties to reduce the risk of fraud.

- **Transfer the risk**. Having a third party assume the consequences of the risk. In most cases, only part of the risk is transferred. For example: insurance (payment of a premium against compensation in the event of a claim), transfer to banks when borrowing, contractual measures with customers or suppliers. Responsibility may be partially transferred by delegation of authority or contract, but not the main responsibility to the customer. The term "shared responsibility" is more appropriate. It should be noted that image, legal and human impacts are not generally transferred to third parties because they affect the Company's liability.
- **Sharing the risk**. The risk can also be shared with associates or partners: for example, local partners who will share the operational risks on a construction project, or co-shareholders in a JV.
- **Accepting the risk.** Doing nothing is a possible option. However, it implies that the level of risk can be measured and contained within acceptable limits, and that the action plan is effective and appropriate. This is also known as risk retention.

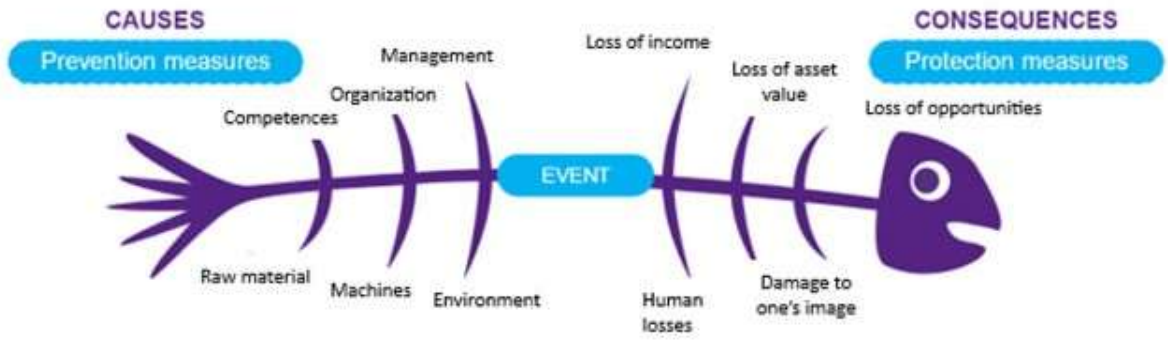
Strategic risks are risks linked to the notion of entrepreneurship. They cannot be reduced or transferred like operational risks.

They can also be dealt with through innovation, adapting business models, lobbying, economic intelligence and skills development, for example.

The mitigation strategy is often a combination of the various basic strategies.

It is sometimes possible for the Group to opt for other mitigation strategies: increased risk (excessive caution in the past, changes in the context, in technology, etc.), adaptation of its business model, etc.

Depending on the mitigation strategy chosen, action plans will be defined and implemented to achieve the target risk level. This will be based on an analysis of the causes and consequences in order to select the appropriate measures:



The pertinence of the mitigation plan must take into account the cost/benefit ratio: Management may therefore be led to accept a risk if the cost of its mitigation is deemed too high in relation to the expected benefit.

Finally, when the uncertainty or the measures put in place can have a positive aspect, it is important to take this into account in order to adapt the mitigation and the target level. Action plans and mitigation plans can also create **opportunities** that go beyond reducing the level of risk. Where this is the case, the description of the risk will be supplemented by a description of the associated opportunity.

2.4 Monitor and review risks

The mitigation plan consists of:

- continuous actions to move from the inherent risk to the residual risk, and
- specific actions, defined over time, which enable the inherent risk to be reduced to the residual risk and, in some cases, the level of residual risk to be brought up to the level of the target risk.

The progress of a mitigation plan must be objectively measurable: quantitative indicators or key progress milestones must therefore be defined when the mitigation plan is put in place and be the subject of periodic progress reviews.

In addition, it is recommended that a system be put in place to enable the actual effectiveness of the mitigation plan to be assessed in the light of changes in the indicators used to assess exposure to risk.

We recommend using existing operational indicators (e.g. customer satisfaction rate, asset availability rate, opinion poll, financial indicators, etc.).

The Internal Audit, Internal Control and Risk Management may usefully be consulted to give an opinion on the quality and effectiveness of the mitigation plan.

In summary, an effective mitigation plan requires to have defined / put in place:

- a target risk objective,
- identification of the main risk factors and definition of an associated mitigation strategy,
- a pilot for each action to achieve the target risk level,
- monitoring the implementation of mitigation plans.

The quality and effectiveness of the mitigation plan for each risk is assessed on a four-point scale, as follows:

Quality	Decided strategy	Implemented strategy	Comment
To (re) build	No	No	This may be the case for a new risk or if the risk exposure has changed significantly. The risk management strategy is not yet defined or redefined.
Low	Yes	No	This may be the case for a risk that has already been identified but whose scale or nature has changed. The strategy is defined but not implemented. The mitigation plan or monitoring system is not yet implemented.
Perfectible	Yes	Partially	A mitigation plan is in place but is not sufficient for the target risk or is not yet fully implemented.
Good	Yes	Yes	The defined mitigation plan is sufficient and appropriate to achieve the target risk. The treatment plan and monitoring system are implemented.

CHAPTER 3: AN OPERATIONAL ERM

For the ERM review, two combined approaches are deployed within organizations:

- The "Top-Down" approach is a flow of strategic information that starts with the vision of BoD / Executive Management: it structures the vision of risks and provides the broad guidelines to be taken into account by the operational entities in their work;

  The CRO organizes an exercise to identify the Group's macro-risks, starting with a review of the summary of Group's risks by the Board and continuing with a "Top-Down" exercise in the form of interviews or brainstorming with the members of the Executive Committees.

  The most important risks for which Management would like to have an overview, including risk scenarios and mitigation plans, are highlighted.

- The "Bottom-Up" approach is a flow of operational information based on the vision of the Entities / Operations on the ground: they report risks linked to specific operational situations.

First year implementation

Organized by the CRO / CFO at HQ, this **Kick-Off** formalizes the start of the risk review. The Group's risk analysis instructions are then sent to the subsidiaries:

- the specific guidelines set by the Executive Committee and reviewed by the Group Audit Committee for the first year. They may lead to certain risks or risk categories being examined in greater depth for cyclical reasons;
- the risks identified during the Top-Down analysis;
- the specific risk analysis instructions defined by the various functions (i.e. HR, legal GDPR, IT), lines of defense (Internal Audit).

Exchanges with the various subsidiaries and CRO

During the review, it is essential for the CRO to maintain regular communication with various contacts within his/her entity, in particular:

- the various "functions" and operational activities, in order to identify risks, make the best possible assessment of inherent and residual risks and define risk scenarios, as well as challenging the action plans proposed by Management,
- the other lines of DEFENSE (internal control, internal audit) to help assess the effectiveness and impact of the action plans,
- to keep the CEO informed of the progress of the review.

Note: It is advisable to document the assessments in the same formats as soon as possible. All the quantification details are carried out as soon as the necessary data is available.

If necessary, the CRO can aggregate risks of the same nature, having the same causes (to bring together a

common lever on prevention), or the same consequences (to bring together a common lever on protection), or to group together certain risks of low importance, but recurring in several entities (risk having the same business issues or the same identified risk owner).

Summary of Group's risks

The purpose of the risk review is to enable the Entity's Board or Executive Committee to:

- validate the overall risk exposure (short-, medium- and long-term) that the entity accepts in the light of its objectives, the Group's risk appetite policies and changes in its environment,
- steering the main risks by monitoring their development, implementing mitigation plans and appointing risk owners,
- assess the effectiveness of mitigation plans and decide whether to adapt them,
- identify emerging risks at entity and country level,
- informing stakeholders about these risks,
- communicate the risk culture at all levels of the organization.

The final deliverable is also presented to the Board and Audit Committee at a meeting attended by the CRO, CFO and CEO of the Entity.

Prioritization and selection of risks to be considered in the review

Once the analysis of individual risks has been finalized, and with a view to preparing the review of the entity's risks, the CRO prioritizes the risks and selects those that will receive particular attention.

It is recommended that a maximum number of risks be selected at entity level (corresponding to a Top10 or Top15), at country level, to make risk analysis easier to understand and to prioritize action plans.

It is recommended that the Executive Committee have an informed debate based on objective criteria:

- **Financial impact** on results,
- **Non-financial impact**, particularly with regard to stakeholders,
- **The sustainability of extreme scenarios**,
- **The evolution and degree of risk management** (quality and effectiveness of mitigation plans).

They also meet the compliance and governance needs of listed companies and provide transparency in the external communication of listed companies' risks (annual report).

Risk matrix and global overview

The risk matrix gives a global overview of all the risks for a given perimeter. Each risk is positioned on the standard likelihood/impact map. The coordinates of the point representing the risk are its likelihood on the x-axis and its total impact on the y-axis. The background colors on the map have no other meaning than to guide the reader.

LIKELIHOOD	INSIGNIFICANT	MINOR	SIGNIFICANT	MAJOR	CATASTROPHIC
CERTAIN	Low	Moderate	High	Extreme	Extreme
LIKELY	Low	Moderate	High	High	Extreme
POSSIBLE	Low	Moderate	Moderate	High	High
UNLIKELY	Low	Low	Moderate	Moderate	Moderate
RARE	Low	Low	Low	Low	Low

IMPACT

The matrix allows you to:

- put all the information into perspective in a graphical format,
- identify the most significant risks by presenting a cross-cutting summary of risks ranked in order of importance at a given point in time,
- gain a deeper understanding of the risks and, if necessary, identify dependent or interlinked effects (domino effect) and thus optimize mitigation measures and action plans,
- check the adequacy of control systems in relation to these risks,
- provide a basis for effective internal risk communication.

Coordination of budgeting process and global risk management processes

The final review of the Entity's risks is carried out in accordance with the budgeting process: risks are quantified with reference to the Entity's budget.

- High probability risks (>50%) are included in the budget (at least in part). At the very least, they should be discussed at the annual review;
- the costs of risk management plans are included in the budget.

CHAPTER 4: RISK CATALOGUE

Appendix 1: risk catalogue – excel format. Some examples below.

Strategic risks
• Business environment / Competitors • Regulatory environment • Reputation and marketing strategy • Definition and analysis of the general strategy • Reaching development ambitions • Organizational design • Investments and acquisition evaluation & post-acquisition integration
Financial risks
• Interest rates and exchange rates • Liquidity risk • Financial and/or commercial counterparty • Pensions and retirement schemes • Other financial risks (impairment, ...)
Operational risks
• Efficiency, performance and maintenance of our operational activities • Patient treatment • Infections • Quality / Technology • Loss of competences / Retention / Churn • Employee involvement / stress / disengagement • Labour relationship / social climate • Digital transformation of processes and data usage • Cybersecurity of IT infrastructures, industrial control systems or business applications • Availability of internal information systems or external IT suppliers • Physical risks related to climate change • Natural disasters (except climate change) • Corruption and other ethics & compliance violations • Non-compliance to local data privacy regulation (GDPR) • Purchase and Supply Chain • Health and safety • Security • Waste management