1

Introduction to Risk and Risk Management

Risk management is undoubtedly one of the most frequently used phrases in the current social and economic scenario, the importance of which has progressively expanded in line with the regulatory evolution which, in a consolidated manner, has taken on risk and its management as a criterion for the responsibility of the individual and the organization.

Apart from the subject of the interaction between the evolution of regulations and the development of risk policies, it can certainly be said that risk management is now an integral part of company processes, not simply as a legal necessity but increasingly as a factor and opportunity for consolidation and development of the organization and production processes.

From this assumption emerges the need to focus attention on risk management methods, not so much to find a definition – which, although effective, would not offer great applicative utility – but to substantiate its implementation with methodologies able to offer logical coherence to all phases of the process.

Completeness and effectiveness of risk management are in fact directly correlated to the capacity of the process to develop in phases and levels directly related to the articulation of the organization and the processes analyzed.

Considering the complexity and operational breadth of the company organizations, and therefore the network of processes, both internal and external, that condition the pursuit of results, it is quite clear that the risk management process is not immune from the risk of losing coherence of the parameters adopted in the analysis, altering the outcome of the assessment and jeopardising the possibility of consistent revision in the updating and comparison phases.

Of course, managing risk is not a question of "harnessing" it through the search for aprioristic rules that limit its potential in terms of flexibility and adherence to the specific realities analyzed, which is – a bit simplistically but effectively – the added value of the process.

It is only a matter of identifying methodologies that assist the development of risk management in a flexible but coherent manner in all phases and levels, guaranteeing its analytical and evaluative rigour, and its applicative and comparative replicability, ensuring its effectiveness with respect to the complexity of modern organizations and the network of relevant processes, in an organic vision of organizational, technical and management factors.

Bow-Tie Industrial Risk Management Across Sectors: A Barrier-Based Approach,
First Edition. Luca Fiorentini.

Risk management can have variously articulated perimeters and purposes of analysis.

Consider, for example, the risk linked to the safety management of a production unit located in a single location, on the outskirts of an average provincial town, characterized by a single operational process and in a context in which no interference between production processes belonging to different employers takes place.

Imagine instead the same production unit that is part of a wider production organization, belonging to a holding company that splits the operating processes between several subsidiaries, relocating them to several plants where different employers operate with interference between their respective suppliers.

Again, consider the hypothesis that the corporate development indicated above leads to the location of the production unit in the context of complex infrastructures in which several owners/managers/employers subject to different reference regulations operate, and not always coordinated from a technical and managerial point of view, such as, for example, in airports and railway stations where, moreover, the presence of third parties (the public) is predominant; to be practical, think of the employer of a catering activity within an airport.

The perimeter of the risk analysis would seem to be limited in the first case, that of the single production unit; moreover, the identification of processes relevant to risk management would be reduced to the only production process located in the production facility.

The perimeter of the analysis is more articulated in the second case and enormously more complex in the third.

But what would happen if, in the single production unit of the first case, radiographic materials or highly harmful chemical products were treated?

The perimeter of the analysis would be unchanged from a strictly technical point of view, although considerably more complex; the management profile would instead be enormously more complex and open to external factors where it is generally considered, in force of the law, that the employer must take appropriate measures to prevent the technical measures adopted from causing risks to the population or deteriorating the external environment by periodically checking the continued absence of risk.

But let us return to the catering production unit where the parent company, as in the second case, has introduced the administration of different product lines belonging to different subsidiaries and outsourced, for the common benefit, the cleaning and maintenance services of the common food court and the internal spaces in the legal availability of the individual subsidiaries.

The development has preserved the technical risk factors, implementing the management ones from the point of view of interference in operational processes and communication and coordination costs.

Finally, it is clear that the complexity of the risk management process is accentuated when our catering production unit moves into the station (equally, albeit on a smaller perimeter, where it moves into a multiplex cinema or shopping centre).

The technical and management process, and the corresponding risk factors, is significantly extended in correspondence with the management of the station premises, where other commercial, service and railway production units operate alongside the catering unit, without prejudice to the presence of the public.

The catering unit, like the others, is the bearer of the management of its own risks, which must be coordinated with those of the other production units.

But the same production unit is the client of the initial set-up of the space in use and the service and maintenance activities of the same, in which, however, it interferes with the supply of condominium services provided through other contractors on behalf of the station manager.

Likewise, again with regard to safety and fire prevention, the fitting out and operation of the unit must remain consistent and coordinated with the fire prevention design of the station, which in turn is developed in primary and secondary activities included in the building complex.

It is also necessary to consider the hypothesis in which the controlling company of our catering production unit arranges for the sale of products and the size of the space in use to make the point of sale subject to fire prevention controls with the need to coordinate, also in terms of time, the relevant documentation of the single unit with that of the station.

All of this is articulated in an extensive activity of cooperation and collaboration that sees the relationship between the station manager and the manager of the production unit installed, with charges of promotion of coordination from time to time with the client or promoter of the modification, management and coordination of the risks introduced, and relative diffusion to the other parties for the corresponding evaluation from the point of view of their respective interests.

Furthermore, development of the same process occurs over time in relation to the changes made from time to time by each of the parties in question (set-up, entrusting of services and works, etc.) and the repetition and updating of the cooperation and collaboration process described above.

To further accentuate the complexity of the process, consider the need for the station manager to guarantee adequate safety conditions with respect to third parties present in the station for whom there is no margin for process management other than those limited to signage in the areas.

Irrespective of the "colour" with which the three conditions represented above and the deliberately simplistic nature of the relative characterization have been represented, it undoubtedly emerges that risk management, already with respect to the technical and managerial safety profile alone, is a multi-stage process (work safety, fire prevention, administrative requirements, etc.) and is carried out on several levels of interaction between different but mutually relevant and interfering subjectivities.

In this sense, the need for a methodology that organically covers the different phases and connects the different levels with logical consistency and applicative replicability, also for updating and comparing the results in relation to the changes that have occurred, appears evident and of pressing necessity in order to guarantee the complete mapping of technical and management activities in the reciprocal interferences.

In the three cases represented above, with the development of our catering unit, no reference was made by chance to the decisions of the controlling holding company.

Paradoxically, and in purely theoretical terms, the scope of risk management analysis could be extended to infinity or almost infinity; to confirm this, we reiterate the need for a methodology that assumes consistent parameters and replicates them in all phases of the process.

Some correlations are, however, directly formulated by the legislator, where it provides (e.g. some specific regulations on industrial risk management) that the risk of the technical

and management process goes back to the body in terms of responsibility, or when the body itself is presumed to be exempt from responsibility where it has adopted and effectively implemented an organization and management model ensuring a corporate management system with respect to specific obligations.

In addition, perhaps even more explicitly and with reference to security processes, the importance of organizational factors is laid down in the text of other Italian laws, which states that "the guarantee positions [...] also apply to a person who, though not having a regular office, actually exercises the legal powers relating to each of the persons defined therein."

In other words, and with reference to corporate risk management, organizational factors cannot not be included in the risk management process, even if it is from time to time aimed at more specific profiles such as safety or environmental risk assessment or in terms of sustainability.

Just think, for example, of the case in which the company organization divides management and commercial competencies and top management entrusts the safety function delegations to the manager in charge of management.

Any misalignment of processes shall not correspond to the same responsibilities with respect to any non-compliance.

In other words, with the risk management processes, the possibility of instrumental use of function delegations is in some way undermined and the assessment of risk as a criterion for making the organization responsible refers to the more detailed analysis of the consistency between organization and responsibility.

The above considerations, albeit in a concise and in many ways summary manner, are intended solely to highlight the assumption that risk management, due to the importance assumed in the current regulatory framework and the complexity of the reference scenarios, is required to be based on methodologies capable of replicating logical and evaluative consistency in all phases and levels of the process, regardless of the scope of the analysis.

With these premises, this book is intended to be a valid reference, for professionals and technicians in the risk management sector, to the rigorous approach of barrier-based risk management. The basic idea behind this approach is to integrate the traditional and well-defined risk management processes using a barrier-based perspective; basically, the one suggested by James Reason with his well-known Swiss Cheese Model (Reason, 1990) (Figure 4).

This integration leads to value-added risk management that, if pursued in every direction, becomes the solid foundation on which to build enterprise risk management (ERM). Several books have already been published on similar topics. This one wants to implement these key concepts in the daily business of every organization by transferring this information with the help of two barrier-based methods: Bow-Tie (BT) and barrier failure analysis (BFA).

Their advantages and disadvantages will be discussed in-depth, as well as how to create, step-by-step, a typical Bow-Tie and BFA diagram, regardless of the business sector of application.

The intentions of this book are:

- To present the contents of the technical standards about risk management (ISO 31000, *Risk Management – Guidelines*; ISO, 2018);
- To give a solid introduction to enterprise risk management (ERM) across different industrial sectors;

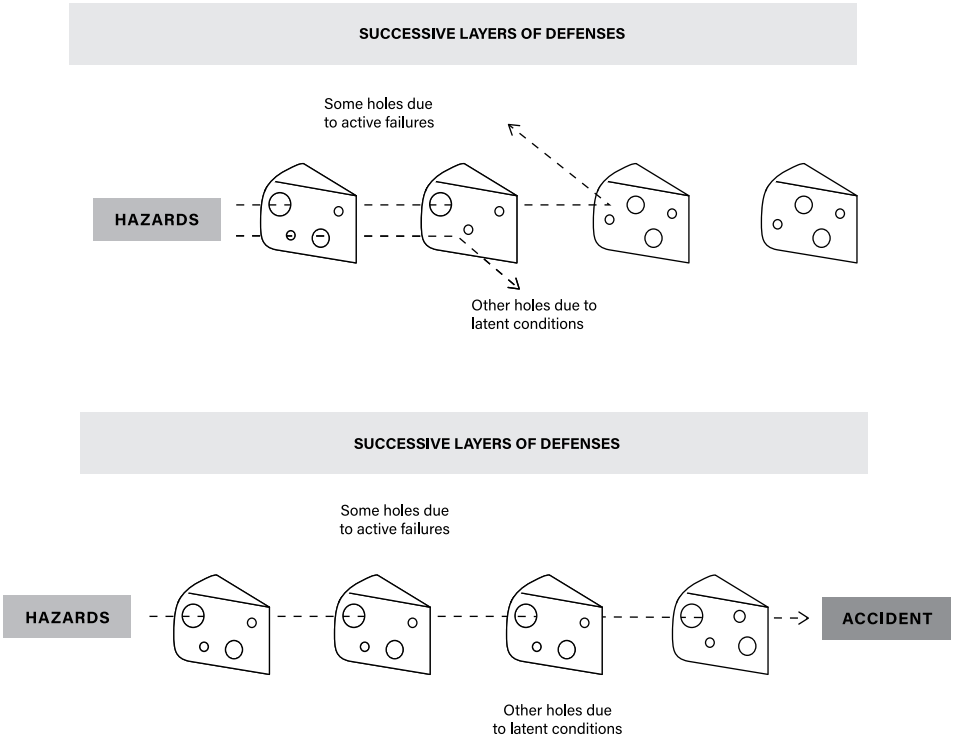


Figure 4 Swiss Cheese Model. *Source:* Reason, J., 1990.

- To suggest a risk-based perspective for some ISO standards;
- To introduce the barrier-based approach to risk management;
- To present the Bow-Tie method, its history, its elements, and how to get value from its implementation;
- To present barrier failure analysis, its elements, and how to get value from its implementation;
- To show how it is possible to link proactive and reactive phases of risk management (RM) using these methods;
- To offer some worked examples of both Bow-Tie and BFA methods;
- To help the reader with a step-by-step guide on how to implement the two methods.

The Bow-Tie method is widely adopted in the process industry, where it was born, and it has been developed to deal with industrial risks. This explains why some guidelines mentioned in this book, as properly referenced, come from the American Institute of Chemical Engineers – Center for Chemical Process Safety (AIChE-CCPS, 2018).

The first chapter is dedicated to a general introduction to risk and risk management: the ISO 31000 standard is presented, with its framework and process. The second chapter is where the Bow-Tie method is deeply discussed in theory, also showing some advanced usages; similarly, Chapter 3 is for BFA. Chapter 4 describes the Bow-Tie and BFA construction workflows with step-by-step guides; the layer of protection analysis (LOPA) construction

workflow is also described. This chapter also contains some real case studies coming from several business sectors (Oil & Gas, Food Industry, Healthcare, Transportation, and Energy, just to mention a few). After the Conclusions, three appendixes end the book: the first two are simple, supportive material that the risk analyst or the incident analyst can use as a few-pages guide where only the key concepts are expressed, just as a fast refresh tool. A short presentation of the Human Error and Human Reliability Assessment is in Appendix 3.

Throughout this book, a consistent vocabulary is used to avoid any misunderstanding in using extensive and complex terminology. The main reference for this is ISO Guide 73, *Risk Management – Vocabulary* (ISO, 2009).

The following list is a glossary of the main terms used.

- *Risk:* Effect of uncertainty on objectives (either positive or negative deviation from what is expected). Often expressed as a combination of the consequences of an event and the associated likelihood of occurrence.
- *Control:* Any measure or action that modifies risk. It includes any policy, procedure, practice, process, technology, technique, method, or device that modifies or managed risk. Risk treatments become Controls or modify existing Controls once they have been implemented.
- *Risk Source:* Where a risk comes from. It has the potential to generate a risk.
- *Hazard:* A source of potential harm; present condition, event, object, or circumstance that could lead to or contribute to an unplanned or undesired event such as an accident.
- *Issue:* Risk with a probability of occurring of 100%; that is, it has eventuated into an existing issue.
- *Risk Assessment:* Process that is made up of risk identification, analysis, and evaluation.
- *Risk Identification:* Process of finding, recognizing, and describing risks involving the identification of risk sources, events, causes, and potential consequences.
- *Risk Analysis:* Process to comprehend the nature of risk and to determine the level of risk.
- *Risk Evaluation:* Process used to compare risk analysis results with risk criteria to determine whether a specified level of risk is acceptable.
- *Risk Treatment:* Process to modify risk that can involve avoidance, taking or increasing risk, removing the risk source, changing the likelihood, changing the consequences, sharing the risk, retaining the risk by informed decision.
- *Residual Risk:* Risk remaining after risk treatment.
- *Consequence:* Outcome of an event and affects objectives.

For the purposes of this book, it is assumed that the reader knows that risk is different from a hazard (the risk is the future impact of an uncontrolled hazard or, better, the future uncertainty created by the hazard). This is a fundamental difference since all methods are intended to assess the risks associated by inherent methods.

1.1 Risk Is Everywhere, and Risk Management Became a Critical Issue in Several Sectors

No human activity is risk-free. Its definition, so intimately connected to statistical and probabilistic assessments, imposes that the "risk zero" does not exist. Keep in mind that any business activity carries a risk of an entrepreneurial nature, that is, the inherent

challenge of succeeding or not in that business. But, of course, there are also other types of risks that an entrepreneur must pay attention to, including operational, health and safety, environmental, and reputational risks, to name a few.

However, considering the presence of risk to be limited to entrepreneurial activities would be a mistake. In everyday life, we take opportunities by taking risks. There would be no opportunity to cross a road without running the risk of being overwhelmed by a running car, of driving a car without running the risk of going off the road, of undergoing medical treatments without running the risk of their failure and being ineffective, even of getting married without running the risk of having to face a divorce. Risk is everywhere, just looking at reality from a different perspective, as long as this change of point of view does not generate anxieties or fears, but calmly allows the acceptance of a true and incontrovertible fact: risk zero does not exist.

As shown in Figures 5 and 6, there is clearly no limit to the applicability of the concept of risk, which can also be scaled to a global dimension. For example, the Annual Global Risk Report by the World Economic Forum (World Economic Forum, 2020) lists the main global economic, environmental, geopolitical, social and technological risks perceived as priorities by the sample interviewed. Interestingly, in recent years there has been a greater awareness of the global environmental risks associated with extreme weather events, loss of biodiversity and the failure of actions to address what is known as the climate crisis, for which there is a high perception of risk both in terms of probability and magnitude, although the use of weapons of mass destruction and water crises continue to be of obvious concern from the point of view of impacts.

Developing a good perception of risk is, therefore, a fundamental piece for a more complete and comprehensive understanding of the world around us and its complexity. Indeed, equipping yourself with this awareness is often the key to the success in many organizations, whose managers, playing the role of true leaders, offer their expertise in guiding the organization through risks and opportunities.

Faced with this permeability of any human activity to risk, we understand the importance of risk management, as an operational and directional tool to ensure the sustainability of business processes and, more generally, human actions. Maintaining an "acceptable" (or at least "tolerable") state over time is, in fact, the ultimate goal of risk management, the complexity of which should force the establishment of well-structured processes and models capable of protecting the organization from dangers and finding added value where there is a risk of any kind.

The concept of risk is associated with several considerations. It is generally seen as the likelihood of an event being harmful, the possibility – more or less likely – that a threat exists and that it could harm an organization's objectives. But events can also have impacts that are positive, negative, or sometimes both. Some events bring with them a neutral conception of risk, such as weather forecasts. If these announce a certain chance of rain for next week, then for a farmer, it is an opportunity while for a tourist it is a threat.

From this brief premise, it is understood that it is necessary to detach on the basis of the mere negative conception of risk as a harmful event to marry, whenever possible, a positive vision (an opportunity to be seized) or at least neutral (probability of event). The definition suggested by ISO 31000, therefore, offers a 360-degree view of the concept of risk: "the effect of uncertainty on objectives."

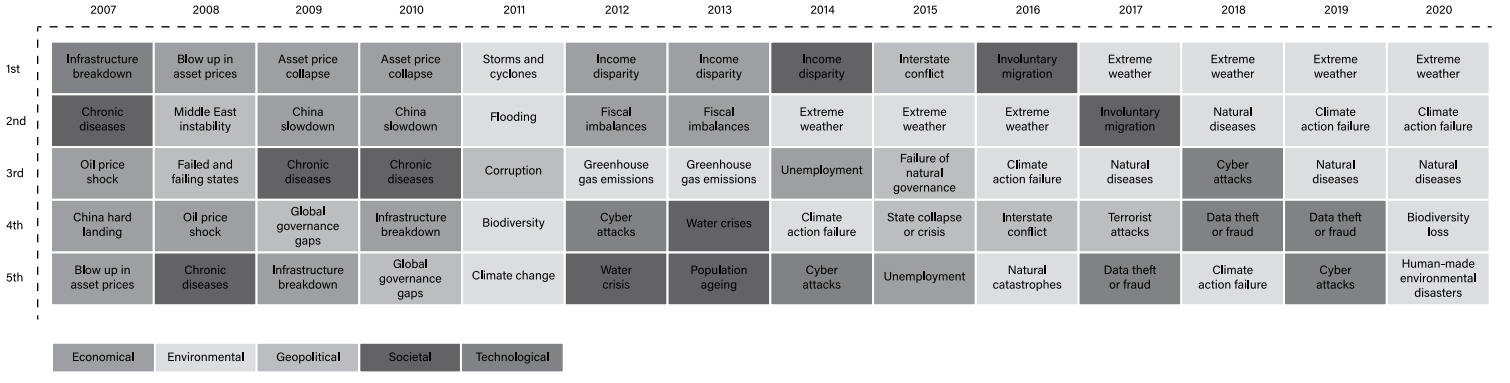


Figure 5 Top five global risks in terms of likelihood (2007–2020). *Source:* World Economic Forum, 2020.

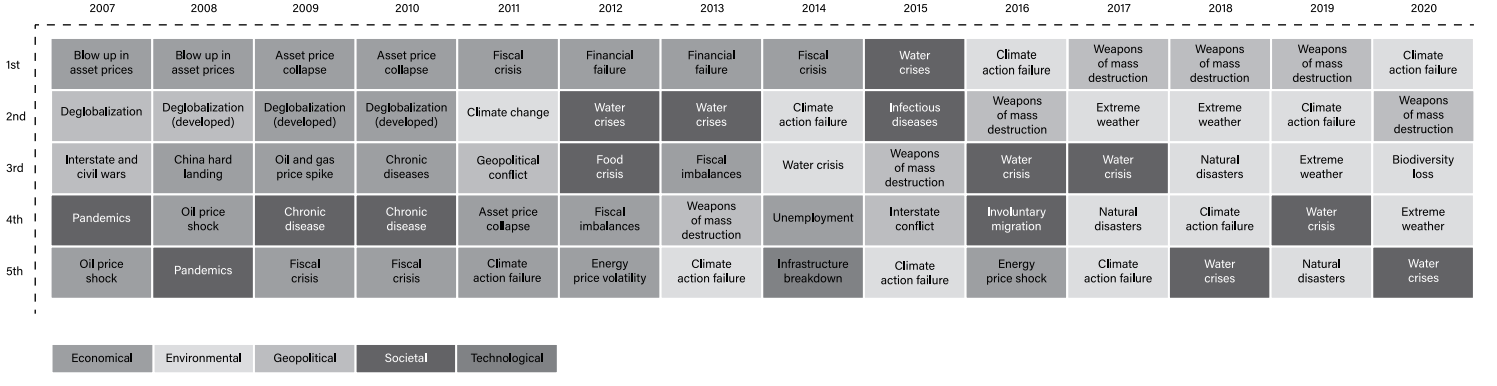


Figure 6 Top five global risks in terms of impact (2007–2020). *Source:* World Economic Forum, 2020.

In relation to the point of view (positive, negative or neutral) with which you look at risk, the organization will set a consequent risk management strategy. From a positive point of view (risk as an opportunity), the organization will tend to maximise the ability to take advantage of the opportunity offered by risk. For example, a lender decides to finance a project and will try to maximize its return on investment. According to the neutral conception, the resulting risk management strategy is to calculate the probabilities of the various risk scenarios and predict their performance. The organization that marries this approach will constantly process reports to monitor and review its risks. If, on the other hand, the view adopted is the negative one (risk as a threat), then the resulting strategy can only be to avoid, transfer, reduce or otherwise not increase the current set of risks. This can be done, for example, by avoiding unsafe technologies, implementing additional control measures, taking out insurance policies and so on.

1.2 ISO 31000 Standard

Regardless of the type, entity, size and complexity of an organization, many regulations and laws (both national and international) increasingly require the adoption of management systems that cover risk management. The adoption of a risk management model that over time complies with the international technical standard ISO 31000 can increase the effectiveness of this action: the organization's efforts are made consistent with a general model that is already consolidated, widely tested and used.

In fact, every organization has to deal with those factors, internal and external to its corporate structure, that make the achievement of its objectives uncertain. In other words, each organization must face its own risks, managing them appropriately in order to ensure the achievement of its objectives.

The ISO 31000 technical standard aims to provide principles and guidelines for risk management. The standard, adopted voluntarily, preserves a universal conception such as making it applicable to any company context, regardless of the nature of the risks associated with the organization's activities, adapting itself in a systematic, transparent and credible way, with the possibility of a progressive approach.

The ISO 31000 technical standard provides guidance to ensure adequate risk management in organizations. The content of the standard applies universally to any organization, regardless of entity, type, business sector and size; for this reason, the indications of the technical standard must then find appropriate customization depending on the specific context of application. Moreover, the document is valid throughout the entire life of the organization, depicting the whole life cycle for risk management. The standard contains proper references that can be applied to any activity within the same organization and embraces decision-making at all levels.

Technical Report ISO/TR 31004 is a valid guide to implementing ISO 31000 effectively. In particular, it provides a well-defined approach to ensure the proper transition, inside organizations, from their risk management arrangement to one that is consistent with ISO 31000. By explaining the underlying concepts of ISO 31000, the Technical Reports offers

guidance to the principles, the framework, and the process described in the standard. These concepts are discussed in depth in the following pages; however, the interested reader is invited to consult both the standard and the technical report to go even deeper and learn extra details that are not treated here.

A third document that every good risk management practitioner has to know is the IEC 31010. This international standard contains a valid guide on the main and well-recognized techniques to identify, analyze, and assess risks. It also offers an approach to the selection of these techniques, depending on some input parameters. However, the document itself contains extra references to other sources that the reader can use to have a detailed description of the methods.

Before presenting the risk management framework, it is necessary to introduce the definition of risk. According to the vocabulary used in the sector worldwide, as stated in the international standards, risk is the "effect of uncertainty on objectives." This definition recalls the necessity to explain what an objective is. An objective, from an organizational point of view, can be defined as the business goals, thus including not only the need to maximize profit, but also the safety goals, reputational goals, environmental goals and so on. Having clarified what risk is, as stated in the previous paragraph, it is clear that risk can be seen from three different points of view (Figure 7):

- Positive view: the risk is seen as a potential gain;
- Neutral view: the risk is seen as the likelihood of events;
- Negative view: the risk is seen as some form of loss.

These three different perspectives reflect different perceptions of the risk. All of them share the occurrence of an event, whose effect can be positive, negative, or both. Indeed, an effect can be seen as a deviation from the expected. This deviation might result in opportunities or threats. In the end, the risk is usually described in terms of hazardous sources, potential events (scenarios), and their consequences and likelihood.

So, having defined what the risk is, the next question becomes: "What is Risk Management?" According to clause 3.2 of ISO 31000, it can be described as the "coordinated activities to direct and control an organization with regard to risk." The expression, widely used both in ISO 31000 and in ISO/TR 31004, refers to the principles, framework, and process that should be set up by every organization in order to manage risk effectively.

Described in this way, managing risks may appear extremely easy; but the reader should take into consideration that the concepts presented here are valid for every kind of organization, regardless of its type and dimension, so inevitably, the description is high-level and needs to be tailored for the peculiarities of each company.

Managing an organization means conducting a series of coordinated activities to direct and control the organization itself, with the unique goal of trying to reach its objectives. Therefore,

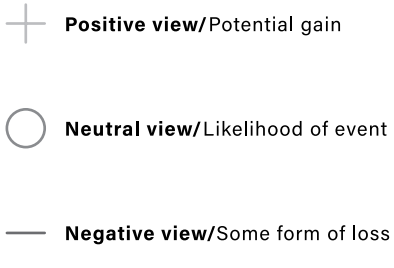


Figure 7 Different perspectives on risk.

risk management is part of management, because it involves the required activities to dominate, or at least control, the effect of uncertainty on those objectives. This is why it is important that risk management is fully integrated into the general management system of the organization; otherwise, its effectiveness is deeply compromised. In this way, it is possible to pursue the risk management purpose, i.e. the creation and protection of value (as stated in ISO 31000, clause 4), improving performance, encouraging innovation, and supporting the achievement of objectives.

Risk management is carried out in the identification, analysis, and evaluation phases, with the aim of identifying any corrective actions that may be necessary to meet the risk acceptability criterion that the organization has set for itself, as well as in relation to any legal requirements. Through this process, the organization communicates with stakeholders and monitors and reviews the risks and control measures put in place to ensure that no further action is needed to reduce the risk levels achieved. This logical process is described in detail by ISO 31000. The standard not only defines the risk management process to be adopted, but also outlines the principles, framework, and workflow that the organization must integrate with its values, policy, and strategy in order to ensure effective risk management and maintain it over time.

The risk management system may apply to all or part of an organization, depending on the objectives and expectations deriving from the application of this management model (Figure 8). For this reason, establishing the context of application of the risk management system represents the "zero" phase of this process: this means not only identifying the organization's objectives, but also the environment in which they are pursued, the boundary conditions, identifying the parties involved, and defining the risk acceptability criterion (or criteria, if diversifying the assessment in relation to the nature and complexity of multiple risks for the organization is intended). This fundamental action is also known as "context analysis."

The relationship between the principles underlying risk management, the framework in which it takes shape, and the operational management process is shown in Figure 9.

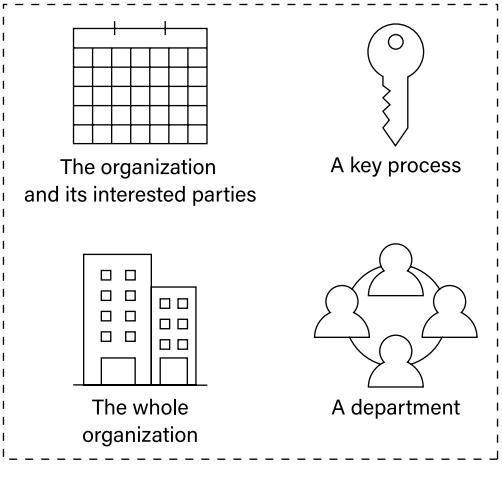


Figure 8 Definition of the scope of risk management.

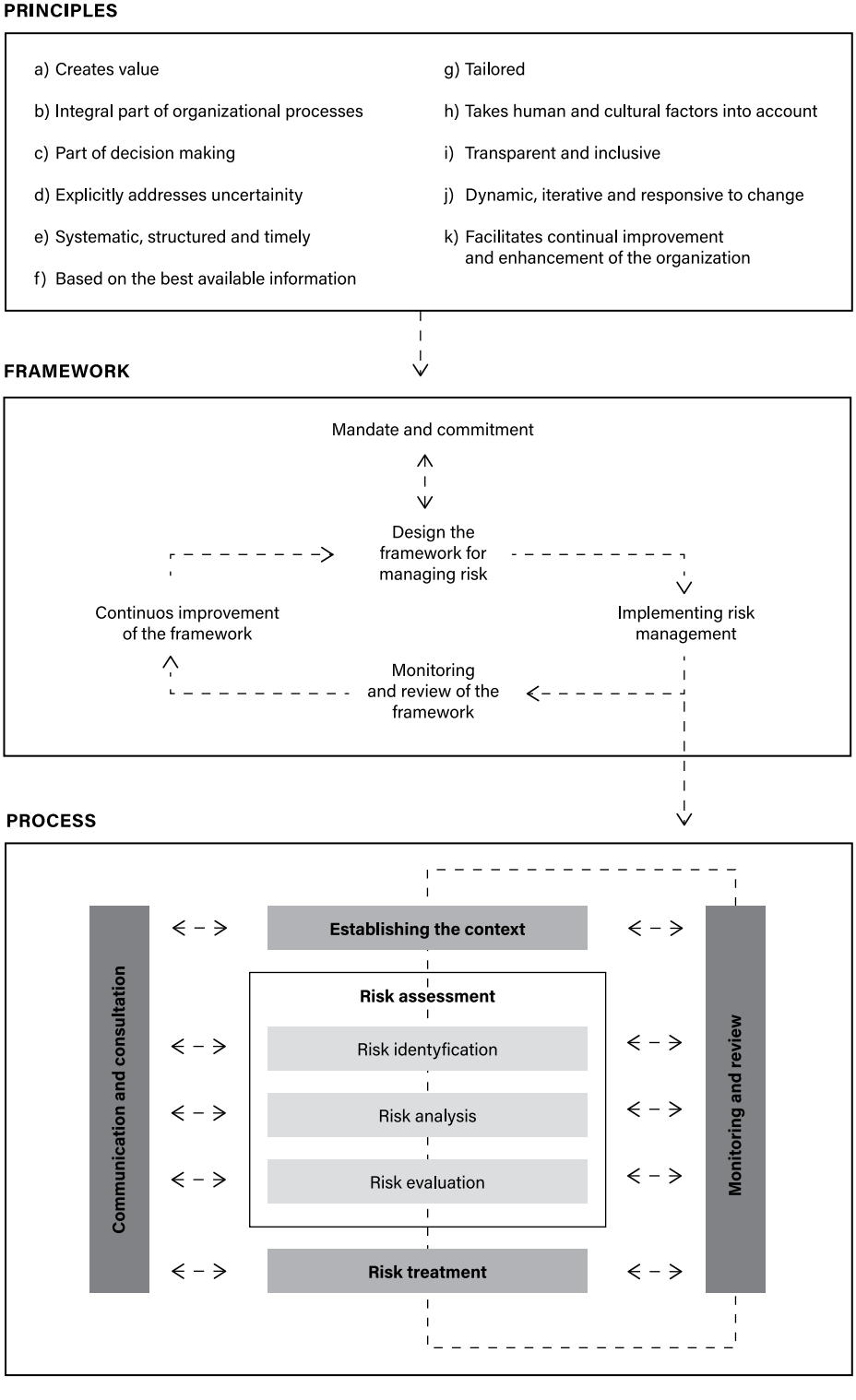


Figure 9 Relationship between principles, framework, and risk management process.

The adoption of the ISO 31000 standard allows each organization to:

- Increase the probability of achieving its goals;
- Encourage a proactive approach to safety from risk (and original hazards), i.e. intervening even before adverse events occur and not only in the reactive phase following an accident, near-miss, or non-conformities;
- Improve the identification of threats to this process and opportunities for improvement;
- Improve reporting activities, whether mandatory or voluntary, and performance evaluation activities through synthetic indicators (KPIs);
- Facilitate the fulfilment of relevant mandatory standards;
- Improve stakeholders' trust in the organization;
- Build a solid management foundation on which to base its decisions and plan its development;
- Improve the internal control system and be able to provide evidence of it;
- Allocate resources (mainly human and financial) efficiently to pursue risk mitigation and ensure over time that the risk reduction factor is identified as necessary;
- Improve operational effectiveness and efficiency;
- Minimize the effects of a negative event, such as an accident, near-miss, or non-conformities (including process anomalies);
- Improve incident management, from the emergency response phase to the investigation and analysis of the incident;
- Improve the exploitation of operational experience, developing recommendations or more general observations, effective as well as based on the "root causes" of and incident;
- Increase resilience.

In few words, organizations embracing a structured approach to risk management have the chance to improve their resilience to complexity and have a higher chance to reach their strategic objectives.

1.2.1 The Principles of RM

When managing risk, it is essential to consider the principles that enable the creation of solid RM framework and processes, allowing an organization to dominate the effects of uncertainty on its objectives. In particular, ISO 31000 defines eight principles that an organization should satisfy, describing the logic behind an effective and efficient RM. Indeed, their satisfaction allows the creation and protection of value, as shown in Figure 10.

Readers should be aware that the most recent version of ISO/TR 31004 goes back to 2013, whereas ISO 31000 was reviewed in 2018; however, most of the principles described in the technical report are well aligned with the newest version of ISO 31000.

To manage risk effectively, each organization should adhere to the following principles at all levels:

- Risk management creates and protects value. In other words, it contributes to the tangible achievement of objectives and the improvement of performance in terms of (for example) health and safety, environmental protection, quality, efficiency and continuity of operations and reputation.

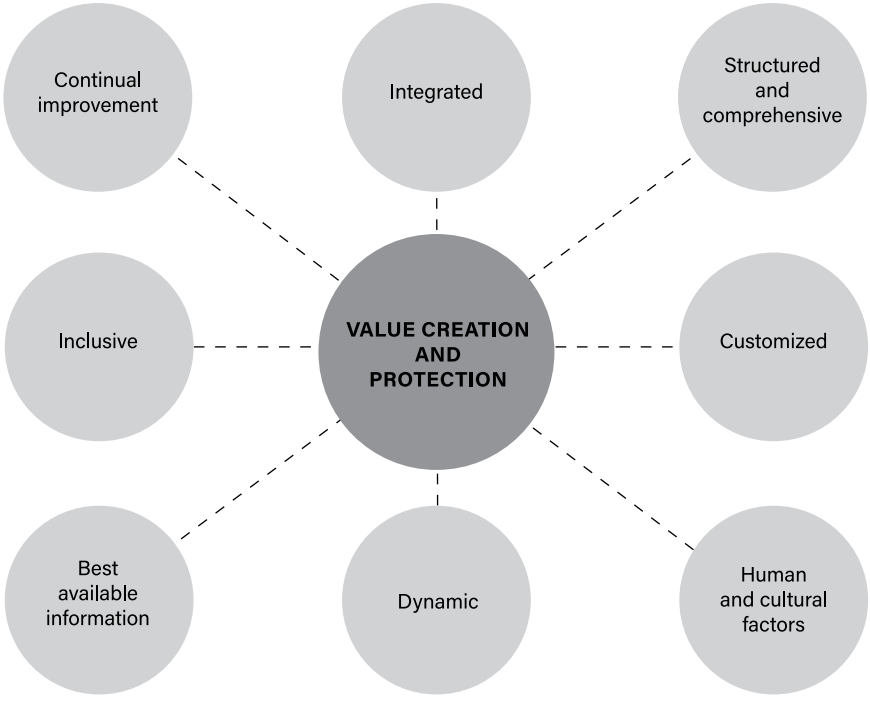


Figure 10 The principles of RM according to ISO 31000.

- Risk management is an integral part of all business processes. It is therefore not a stand-alone activity, but also integrates with project management, management of change and strategic planning.
- Risk management is part of the decision-making process. In fact, it helps decision-makers to make reasoned choices by prioritising the actions to be taken.
- Risk management explicitly focuses on what is uncertain. It is therefore good to be aware from the outset of the role of uncertainty in this area.
- Risk management is systematic, structured and timely. It contributes to operational efficiency and the achievement of consistent, comparable and credible results.
- Risk management is based on the best information available. Stakeholders should be informed of the limitations arising from the information and models used.
- Risk management is tailor-made, taking into account the internal and external context of the organization, including its articulation and complexity.
- Risk management takes into account human and cultural factors.
- Risk management is transparent and inclusive.
- Risk management is dynamic, iterative and sensitive to changes (these in particular must be subject to rigorous management of the change process).
- Risk management helps to pursue the continuous improvement of the organization.

The principles, which are described hereafter, should be tailored to the specific part of the RM framework under consideration and, even if described in general terms, need to be deeply understood and applied continuously to produce the positive effects of an effective RM system.

First Principle – Integrated

Risk management is an integral part of all organizational activities.

RM cannot be considered as a separate part of a management system for an organization, nor an extra administrative requirement or a bureaucratic task, but instead needs to be fully integrated with all the managerial activities in order to create and protect value. This is done by developing the RM framework and applying the RM process to the relevant decision-making and similar activities.

The ISO/TR 31004 suggests how to best apply this principle. In particular it underscores that every decision in an organization bring risks with it, because of the uncertainty that affects both the internal and external context, whose changes cannot be controlled by the organization.

It is not necessary that a management system is formalized in order to integrate the RM. If this is the case, than establishing a RM framework can significantly help. However, ISO 31000 is also a solid reference for existing management processes.

The integration of RM is also fundamental to avoid risks being understood only after that the decision-making process is concluded, thus requiring costly modification in the decision taken and an unacceptable waste of time for competitive companies. In conclusion, it is important to embed the components of RM into the existing (formal or informal) management system, with the same commitment and mandate that are spent for other managerial activities.

Second Principle – Structured and Comprehensive

A structured and comprehensive approach to risk management contributes to consistent and comparable results.

Reliable and successful results can be obtained with a consistent approach to RM. Indeed, satisfying the organization's objectives requires consistent risk criteria that cannot be decided depending on the mood of the day or on the specific needs that may require extra flexibility to reach the goal.

Therefore, RM must consider the time dependencies and be applied timely, at the right moment in the decision-making process; otherwise (if done too early or too late) it could be costly to change direction and the best opportunities could be lost.

The structured approach can be satisfied by the application of the RM process as established in ISO 31000, which suggests the proper activities to be implemented and their sequence.

Third Principle – Customized

The risk management framework and process are customized and proportionate to the organization's external and internal context related to its objectives.

Each organization has its own peculiarities and needs. There is not one specific design and implementation of the RM framework and processes, as they need to be customized for each organization, thus requiring flexibility. Size, business sector, culture, and management approach are elements that need to be considered when defining a way to manage risks.

Indeed, the technical standards that are used as a reference offer a generic approach to RM, being applicable to every type of organizations and risks. The necessity of tailoring the

RM may also emerge within the same organization, when dealing with different risks (e.g. operational, financial, reputational). Systems, methods, and criteria could be different, but the general approach should be consistent and compliant with ISO 31000. Moreover, the designed RM framework should also embed any legal requirements or other external obligations.

Tailoring does not simply mean to change one or more elements of the RK framework or RM processes, as they are described in ISO 31000. It also implies a specific tailoring effort during the design and improvement of the RM framework, not only its implementation. For example, an organization may need to take into account its internal issues like staff turnover or a massive hiring of inexperienced employees who need to be informed and trained on what is required by the RM.

Finally, it must be highlighted that a customized RM framework can be more easily integrated within the general management system of the organization, even if the reverse is always possible, i.e. to modify the decision-making processes to fit the structure of the RM framework.

Fourth Principle – Inclusive

Appropriate and timely involvement of stakeholders enables their knowledge, views, and perceptions to be considered. This results in improved awareness and informed risk management.

The involvement of stakeholders is a crucial point for effective RM. It is therefore important to build trust reciprocally in every step of the RM processes, otherwise some key elements for the design and implementation of the RM could be missed. When implementing this principles, it is important to take into account issues of privacy, security, and confidentiality, so that risk-related information is secured. To do so, it is generally recommended to separate the relevant information in risk registers.

Fifth Principle – Dynamic

Risk can emerge, change or disappear as an organization's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

The environment in which an organization operates is subjected to continuous changes. Those changes in the internal and external context lead to some changes in risks too. Similarly, any modification in the objectives of the organization will change its risks. Therefore, it is important that the RM processes are able to reflect this dynamicity.

The ISO 31000 technical standard explicitly refers to monitoring and reviewing phases for both the RM framework and the RM process. They are two different activities. Monitoring means to observe continuously some key parameters in order to determine whether everything works as intended. Reviewing, on the other hand, is a structured process to check if the hypothesis at the base of the design and implementation of the RM remains unchanged or, if not, a review is required on the resulting decisions.

In conclusion, risks evolve continuously and organizations are far from being static: the RM framework needs to be monitored and reviews periodically, in order to pursue the continual improvement, real paradigm for every management systems.

Sixth Principle – Best Available Information

The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

A correct understanding of a risk comes from the availability of the best available information. Indeed, information and data are affected by a certain degree of uncertainties: to know their sensitivity is crucial to develop clear and precise risk criteria. Every decision-making processes should rely on evidence-based information, but this is not always possible because of restraints on time or resources available. In this case, expert opinions should support the limited information available, always avoiding group bias and other human-related errors for this type of judgement.

Risk-related data help to develop supportive statistical predictions, but past evidence has been shown to not necessarily predict the future accurately. Where there is a lack of information, but there is the evidence of a potential harm, prompt action is required to avoid a dangerous situation escalating in a real risk scenario.

Of course, the design, implementation and improvement of the RM framework is based on the best available information. To obtain the best results, the quality of the data, and thus their reliability and accuracy, should be regularly checked and, if required, a review could be triggered.

Seventh Principle – Human and Cultural Factors

Human behaviour and culture significantly influence all aspects of risk management at each level and stage.

The design of the RM framework should consider the human and cultural factors, i.e. the cultural characteristics and level of knowledge of the involved stakeholders, by obtaining their views and analyzing their features. In particular, among the factors to be taken into account there are: social influences, politics, cultural background, and concepts of time. RM may fail to detect early warnings or recognize complexity, or remain indifferent to others' views. To avoid this, the RM framework designer should ask if the organizational structure is appropriate to the needs of the organization, if the formal accountabilities are clearly identified, if the job descriptions are clear and responsibilities are correctly linked, if the communication channels are effective, if the morale in the organization is periodically monitored, if the recruitment and remuneration policies are clear, if periodical internal and external audits are performed to look for unsafe human behaviours, if the procedures are aligned to the policies, and so on.

Eighth Principle – Continous Improvement

Risk management is continually improved through learning and experience.

The operative experience of the organization offers many inputs to correct the RM and improve the capacity to convert risks into opportunities. Indeed, the continual improvement for an organization is the real driving force of any management system that is based on the well-known Deming cycle, i.e. the continuous loop of the Plan-Do-Check-Act (PDCA) phases, as the RM is.

The continual improvement allows better-informed risk-based decisions to be made, helping to reduce uncertainty in achieving objectives, but overall, this principle allows an

organization to remain alert to new opportunities that may arise both internally or externally, with the aim of improving RM efficiency as well.

Continuous improvement may include improving the quality of risk assessment, improving the RM framework, improving the decision-making process, and extending the range of action of RM, including new activities. What is important is that its goal is clearly identified in the RM policy and communicated both formally and informally.

In order to understand what needs to be improved, an organization should monitor both qualitative and quantitative indicators. Of course, some improvements may require long time to be achieved, such as when a specific budget needs to be allocated. Therefore, it becomes crucial to plan the improvement activities taking into account their priorities and benefits.

The application of the principles of RM, as described in ISO 31000, helps organizations in defining their strategy, achieving their objectives and making informed, risk-based decisions, contributing, in the meanwhile, to the improvement of the management systems.

Each organization should therefore adopt a structured approach to risk management: this is what ISO 31000 calls the framework (Figure 11). It ensures that the information

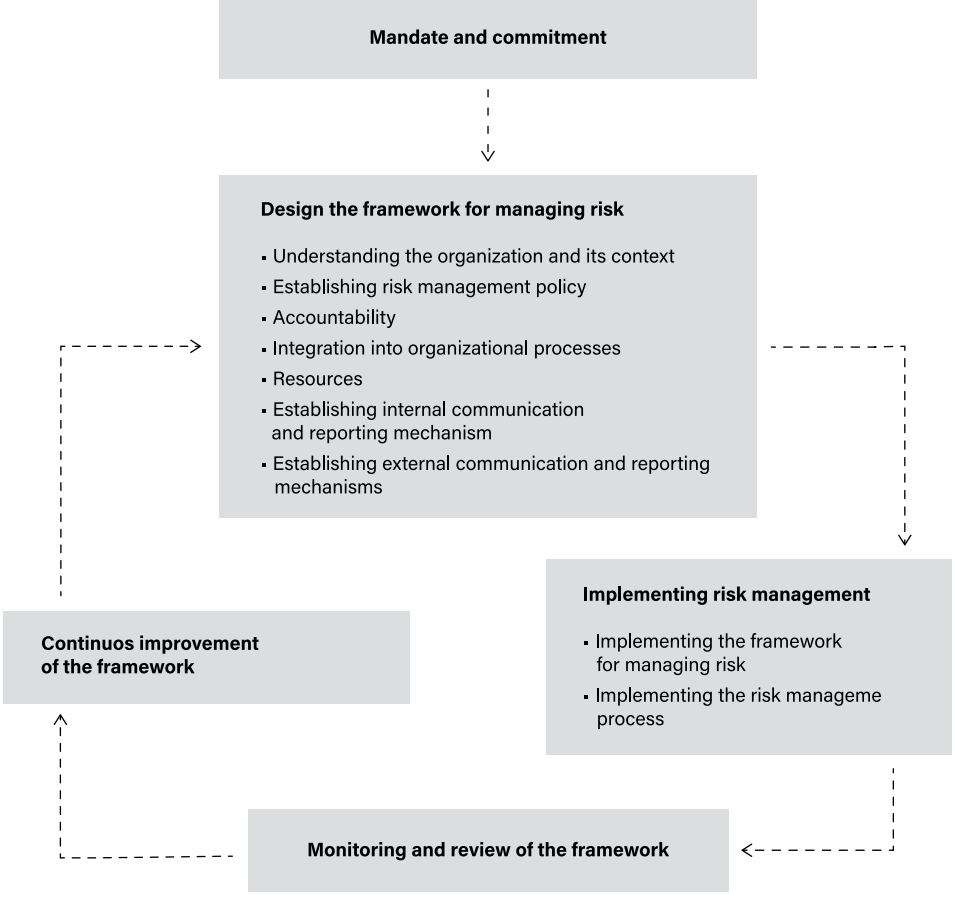


Figure 11 The RM framework.

derived from the risk management process is properly used as a basis for decision-making and the definition of responsibilities at all levels of the organization.

The structured approach to risk management must be based on solid foundations: these are the mandate and commitment, intended as dedication to the cause, of the organization. In other words, this means defining and supporting a risk management policy, ensuring that the corporate culture is always aligned with it. The commitment also implies the definition of performance indicators, strategies and risk management objectives, which must be aligned with those of the organization, always ensuring compliance with mandatory regulations. The corporate mandate requires that responsibilities be assigned to the different levels of the organization, which must also guarantee adequate resources (human and economic) for risk management; communicate the expected benefits of risk management to all stakeholders; and ensure that the structured approach to risk management remains appropriate over time.

Having established the above, it is necessary to design this framework, whose components are shown in Figure 12. To do so, a priority is to know the organization and the context in which it operates, both the external one (social, cultural, political, legal, financial, technological, economic, natural, environmental, international, national, local, etc.) and the internal one (organizational structure, roles, responsibilities, policies, objectives, strategies, resources, information systems, stakeholders, corporate culture, etc.). Knowledge of the organization can also be acquired through the study of company processes and any risk assessments already carried out. The organization's expected risk management objectives

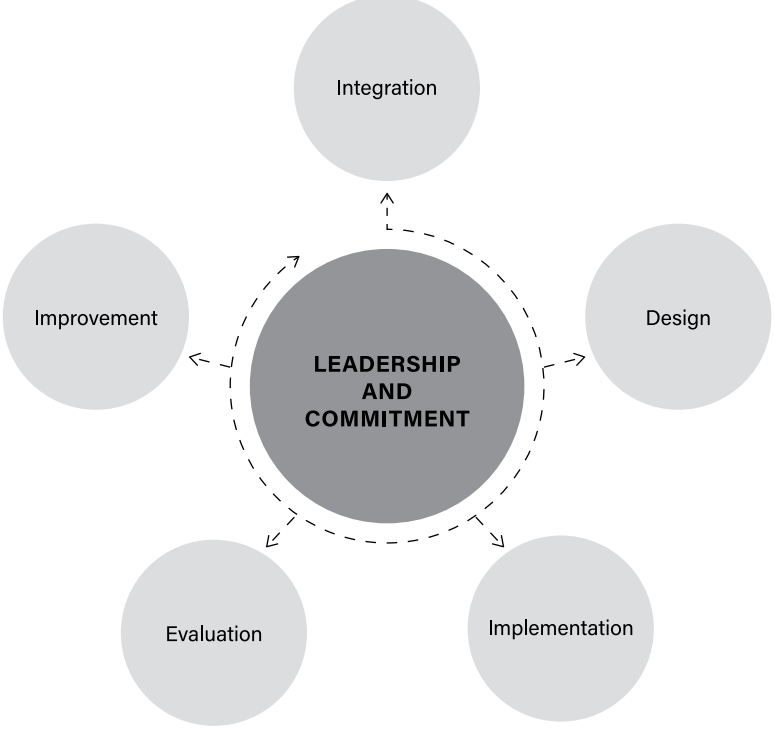


Figure 12 Components of a risk management framework.

must be clearly expressed in a risk management policy document. It must describe how the organization intends to manage risk, clarifying the links between the organization's different objectives and related policies, and also highlight the persons responsible within the organization for such management. A good risk management policy should also indicate how any conflicts of interest are addressed, establish measured performance standards, allocate the resources needed to assist risk managers in their task, and show a commitment to review and improve the policy and framework on a periodic basis or in response to an event or change in the environment. The risk management policy should be communicated in an appropriate manner to all stakeholders.

As part of the structured approach to risk management, each organization must ensure that responsibilities are distributed to the various parties involved in the risk management system, having previously verified that there is the authority to do so, together with an adequate level of expertise in risk management, thus ensuring the implementation and maintenance of the risk management process, and ensuring the adequacy, effectiveness and efficiency of any control measures put in place. This can be facilitated by clearly identifying the individual persons with authority to identify risk management responsibilities, the persons responsible for the development, implementation and maintenance of the risk management structure, and the other responsibilities of persons at all levels of the organization in the risk management process, as well as establishing performance standard metrics and a timely reporting system (also to be understood as documented evidence).

It is essential that this structured approach is integrated into company processes in an effective and efficient manner. The risk management process should be an integral part of these processes, not a separate one. In particular, risk management should be incorporated into business development policies, strategic planning and change management, ensuring that this integration reaches all levels of the organization and is incorporated into business practices, procedures and processes.

The implementation of such a risk management framework requires that the organization allocate adequate resources. In this sense, it would be necessary to question human resources, their skills, experience and competence; the financial resources required by each individual phase of the risk management process; the methods and tools to be used; documented procedures and processes; knowledge and information management systems; and training and updating programmes.

It is also essential to establish communication and reporting mechanisms inside and outside the company context. With reference to the internal context, these mechanisms aim to:

- Support and encourage awareness and understanding of business risks and the assumption of related responsibilities, in order to ensure that the key components of the risk management structure, and any subsequent changes to them, are adequately communicated;
- Support adequate internal reporting on the adopted framework, its effectiveness and results;
- Ensure that relevant information from the application of risk management is available at all levels, at appropriate times according to defined visibility in relation to role and responsibilities;
- Put in place processes of consultation with internal stakeholders in the business environment.

With reference to the external context, each organization should develop and implement a plan on communication with stakeholders outside the company if identified in the context analysis. This translates into a series of appropriately defined activities:

- Adequate involvement of external stakeholders, ensuring an effective exchange of information;
- Production of reports for the fulfilment of legal requirements and possible requirements of the organization;
- Use of communication (including periodic communication) to build trust in the organization and communicate in a structured and shared manner;
- Communication with stakeholders in the event of a crisis or emergency event, providing feedback and adequate reporting on the consultation and communication processes that have been put in place, disseminating information on corrective actions, including preventive ones, defined by a detailed analysis of the root causes and aimed at preventing the repetition of the negative event.

Once the rules with which the organization intends to manage its structured approach (the framework) to risk management have been defined, they must be implemented. In particular, the implementation of the organizational framework dedicated to risk management requires that the organization must, at least:

- Define the timing and implementation strategies.
- Apply the risk management policy and process to business processes.
- Comply with regulatory requirements and any obligations also arising from voluntary adherence to internal or external rules, standards, and best practices.
- Ensure that decision-making processes, including the choice of objectives, are aligned with the results of risk management processes.
- Conduct information and training sessions by implementing an appropriate information, training and education programme.
- Communicate with stakeholders and consult them in advance of key implementation stages to ensure that the risk management structure adopted remains appropriate.

The implementation phase of the framework is followed by the monitoring and review phases of the framework itself, with the aim of identifying opportunities for its continuous improvement.

Once the organizational structure supporting the risk management system has been implemented, it is possible to proceed with the definition of the specific risk management process to be adopted.

The process of communication and consultation with stakeholders is extremely important, as they express their assessments on the basis of their risk perception, experience and degree of involvement in the organization's processes. This perception may vary subjectively due to differences in the values, needs, assumptions, concepts and attention of stakeholders. Because of their potential impact, these perceptions should be identified, recorded and taken into account in the decision-making process. The communication and consultation process should thus facilitate the exchange of true, relevant, accurate, and understandable information, not forgetting aspects of personal integrity and confidentiality.

It is therefore essential to define a criterion to be adopted to assess the significance of the risk even before proceeding with the actual analysis. This criterion must reflect the

organization's values, objectives and resources. Some criteria may be imposed, or derive from legal requirements to which the organization must be subject. The risk acceptability criterion must be consistent with the risk management policy that is defined at the beginning of each risk management process and is continuously reviewed. In defining the risk assessment criterion, the following factors must be taken into account:

- The nature and type of causes and consequences that may occur and how they may be measured;
- The nature and extent of the hazards faced by the organization for each of the processes, products and services to which risk management must be applied according to the defined implementation strategy;
- The way in which the probability of an event occurring is defined;
- The way in which the level of risk is determined (e.g. methodology);
- The stakeholders' point of view;
- The level at which the risk becomes acceptable or tolerable according to the internal and/or external criteria that are applicable for each type of risk;
- The possibility or not of taking into account combinations of multiple risks as well as secondary or "domino" effects, including "escalation factors" that may affect an incidental sequence.

All these concepts are discussed more in-depth in the following section, dedicated to the RM workflow.

1.3 ISO 31000 Risk Management Workflow

As defined in ISO Guide 73, the RM framework (Figure 13) is a "set of components that provide the foundations (i.e. the policy, objectives, mandate and commitment) and organizational arrangements (i.e. the plans, relationships, accountabilities, resources, processes and activities) for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization."

WHAT DOES IT REFER TO?	WHAT DOES IT INCLUDE?	CAPACITY (RESOURCE AND CAPABILITY)
The risk management framework refers to the arrangements (including practices, processes, systems, resources and culture) within the organization's system of management that enable risk to be managed.	The framework includes clear statements from top management on the organization's intent regarding risk management (described in ISO 31000 as mandate and commitment) and the necessary capacity (resources and capability) to achieve this intent.	Capacity does not exist as a single system or entity. Capacity comprises numerous elements integrated into the organization's overall management processes.

Figure 13 Risk management framework.

1.3.1 Leadership and Commitment

Leadership and commitment (Figure 14) ensure the integration of RM into all organizational activities. Indicators that demonstrate the leadership and commitment include:

- The customization of the RM framework components on the specific needs;
- The implementation of the RM framework components;
- The definition of an RM policy, establishing the related approaches, plans, and actions;
- A wide communication of the RM policy;
- The allocation of adequate resources to RM;
- The definition of responsibilities to RM at the appropriate levels within the organization.

Being an RM leader requires solid skills in predicting and accepting changes that may be involved in the behaviour, culture, and processes, and should be reflected within the policy, always monitoring the expected performance while managing risks, and in the RM framework. Of course, meeting the principles of ISO 31000 is among the best efforts for excellence in risk management.

1.3.2 Understanding the Organization and Its Context

In building the risk management process, it is also of paramount importance to prioritize the context (Figure 15).

Its definition allows the organization to articulate its objectives, define the internal and external parameters to be taken into account in operational risk management, and define the scope of the process and the criteria of risk acceptability. These activities are fundamental for the definition of an effective policy. Understanding the external environment is

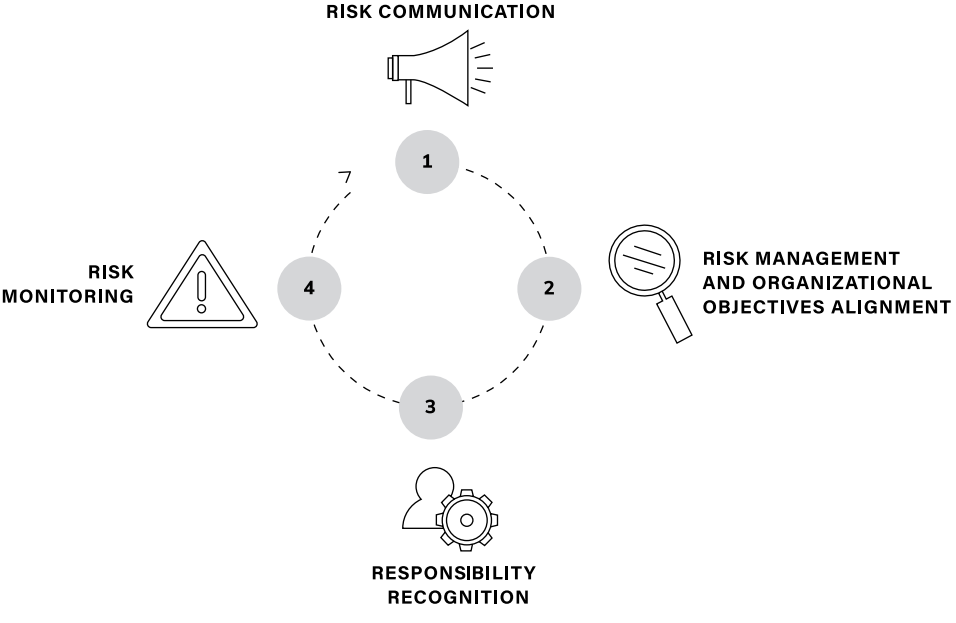
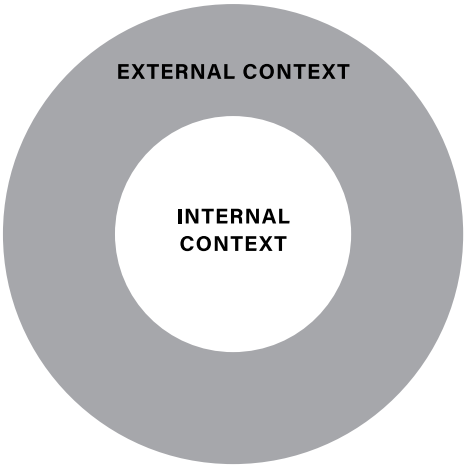


Figure 14 Leadership and commitment.

Figure 15 Internal and external context.



important to ensure that the objectives of external stakeholders are taken into account in the development of risk acceptance criteria. The external environment includes, for example, the social, cultural, political, legal, financial, technological, economic, natural, competitive, international, national, regional or local environment, but also key factors and trends that have an impact on the organization's objectives, relations with stakeholders outside the organization, their perceptions and values. It is essential that the legal requirements and regulations are taken into account when defining the criteria of acceptability and tolerability of risks. The internal context, on the other hand, represents the corporate perimeter within which the organization tries to achieve its objectives. The risk management process should be aligned with the strategy, structure, processes and corporate culture. The internal context includes everything within the organization that may influence the way the organization manages risk. It should be well identified, as:

- Risk management takes place in the context of achieving corporate objectives;
- The objectives and criteria related to the risk management of a particular project, process or activity should be considered in the light of the objectives of the organization as a whole and in compliance with the corporate policy defined by the top management;
- Some organizations are unable to recognize opportunities to achieve their strategic, project or business objectives and this affects the commitment, credibility, trust and value of the organization.

The internal context includes, for example, the organizational structure, roles and responsibilities, policies, objectives and strategies put in place to achieve them, available resources, such as time, capital, human and technological resources, relations with internal stakeholders, their perceptions, values, corporate culture, information systems, information flows and decision-making processes, whether formal or informal, guidelines and models also adopted by the organization through the signing of voluntary commitments. The requirements (both mandatory/voluntary or internal/external) related to RM are shown in Figure 16.

Obviously it is necessary to define the objectives, strategies, scope and parameters of the company activities where the risk management process is applied. This process should be

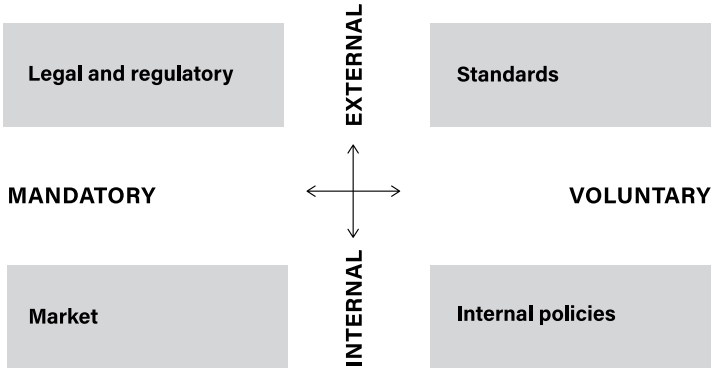


Figure 16 Identify the requirements related to risk management.

undertaken with full awareness of the need to justify the resources employed in the adoption of this organizational model. The context in which the risk management process is applied will vary according to the specific needs of an organization. Its identification may require:

- The definition of the objectives of risk management activities (including the risk aspects towards which the process is directed);
- The definition of responsibilities for the implementation of this process;
- The definition of the responsibilities distributed within that process, i.e. those of the parties involved in that process;
- The definition of activities, processes, functions, projects, products, services or assets in terms of time and space and all those resources that are intended to be used;
- The definition of the relationships between a particular project, process or activity and others within the organization;
- The definition of risk assessment methodologies (even more than one, commensurate with the types of risk and the degree of detail desired);
- The definition of the way in which the effectiveness and performance of the risk management process is assessed (e.g. indicators);
- The identification and specification of decisions to be taken and responsibilities for implementation.

Attention to these and other relevant factors helps to ensure that the approach adopted in risk management is appropriate to the circumstances, the organization, and the risks affecting the achievement of the objectives.

1.3.3 Implementation of the RM Framework

In order to implement the RM framework, an organization should:

- Develop an implementation plan that includes time and resources;
- Identify the features of any decision-making process within the organization (how, when, where, and by who decisions are made);
- Modify the plan if necessary;
- Be sure that the established arrangements (i.e. the RM framework) are clearly understood and put in practice.

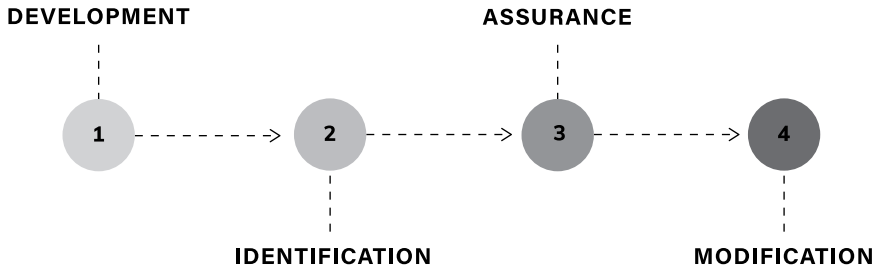


Figure 17 Implementing the risk management framework.

The implementation of the RM framework can be summarised in the four steps shown in Figure 17. It is important to highlight that a properly designed and implemented risk management framework will ensure that the changes in external and internal contexts will be adequately captured, allowing the RM, and by reflection the decision-making processes, to be changed accordingly.

1.3.4 The Risk Management Process

The risk management process should be:

- An integral part of management actions ("management");
- Incorporated into company practices and culture;
- Tailor-made, in relation to the specificity of company processes and the complexity of the organization itself.

This process includes the activities described in Figure 18:

- Communication and consultation;
- Context definition;
- Risk assessment, declined in the phases of risk identification, analysis of the reduction of the risk level starting from the identified hazards and comparison of the calculated risk level with the defined acceptability criteria;
- Treatment of the risk (measures to maintain or develop the level of risk identified, also in relation to the results of the acceptability assessment conducted);
- Monitoring and review.

The first phase of the risk management process is always the communication and consultation with all interested parties, whether internal or external to the company context. In fact, this activity should cover all stages of the risk management process. For this reason, its planning should take place at an early stage of the process. Effective communication and consultation with external and internal stakeholders ensures that those responsible for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions may be required. This approach makes it possible to:

- Better establish the context by taking advantage of the contribution;
- Ensure that the interests of the parties involved are understood and duly taken into account;
- Ensure that risks are adequately identified in a shared and structured way;
- Bring together different skills and experience in risk analysis in order to ensure effective assessment and subsequent treatment;

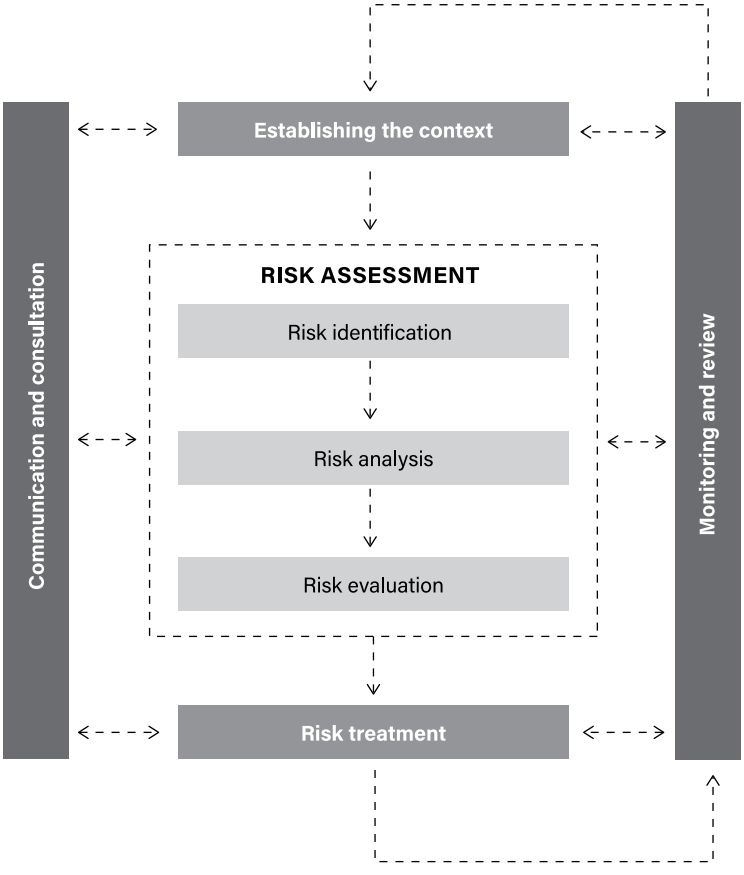


Figure 18 Scheme of the risk management process according to ISO 31000.

- Ensure that different views are duly taken into account when establishing risk acceptability criteria and risk evaluation;
- Develop an appropriate internal and external consultation and communication plan.

1.3.5 Relationship between the RM Principles, Framework, and Process

At the end, the ISO 31000 standard provides:

- The principles;
- A risk management framework;
- A risk management process that encompasses all the vital phases.

An organization wishing to succeed in implementing an effective RM should take into account the relations between them (Figure 19) and apply the principles at all levels; implement an effective RM framework, on the basis of those principles; and apply the RM process (divided in the steps identified by the framework) to the entire organization and modify it to reflect assets and contexts changes.

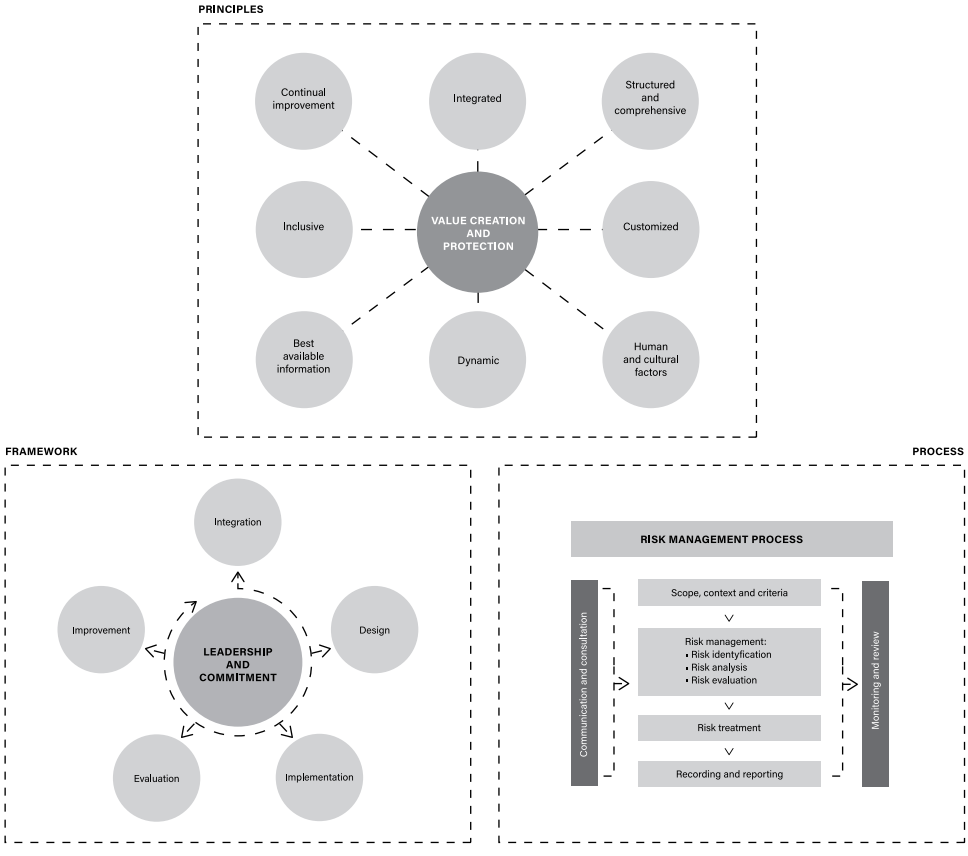


Figure 19 Relationship between the RM principles, framework, and process.

1.3.6 Evaluating and Improving the RM Framework

To evaluate the effectiveness of the implemented RM framework, and help the organization in better achiving its objectives, it becomes crucial to periodically measure its performance and compare it with what was expected. If deviations are monitored, then it is necessary to develop remedial actions to encourage the improvement of the system and facilitate the possibility to take opportunities where risk are present (Popov, Lyon and Hollcroft, 2016) in Figure 20.

1.3.7 The Risk Assessment Phase

Risk assessment is at the heart of the entire management process, as well represented in Figure 21. In particular, once the objectives, criteria, scope and degree of depth have been established, it constitutes the fundamental element for the construction, implementation and periodic assessment of the corporate risk management system. The risk assessment process consists of three phases: the identification of the risk, its analysis, and its evaluation. Some techniques to implement this phase are explained in ISO/IEC 31010 and discussed in the next pages of this book: they are listed in Table 1.

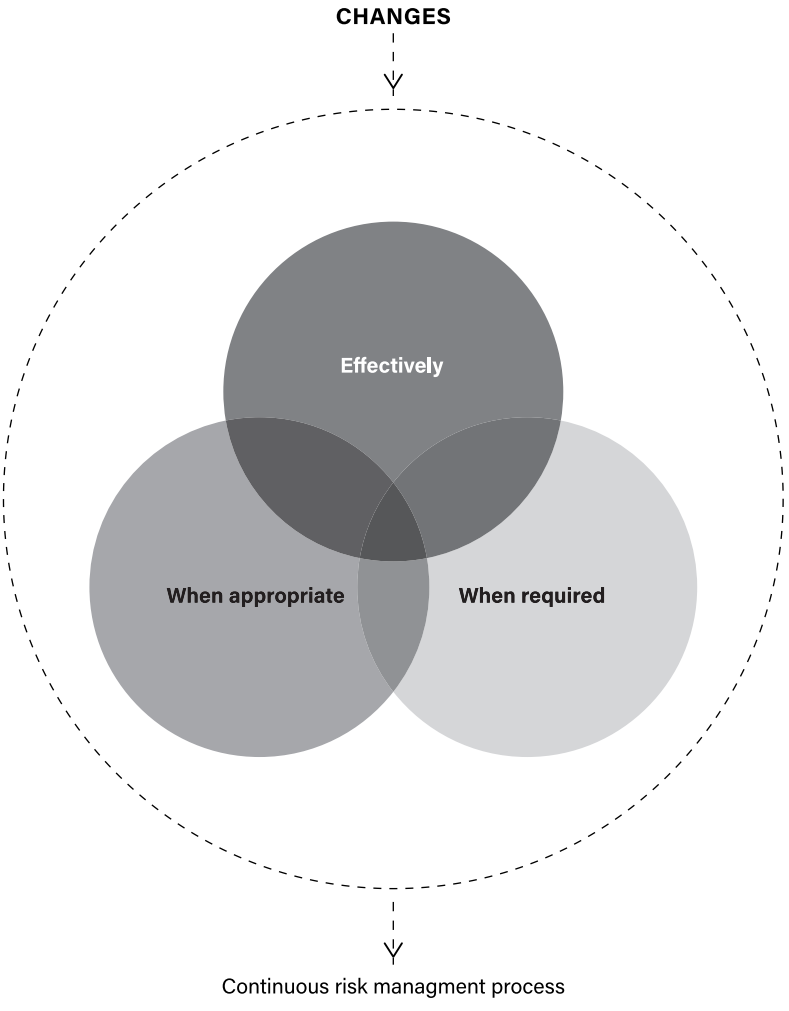


Figure 20 Improving the risk management framework.

This book will discuss some of the methods listed in the table from ISO/IEC 31010, convening a number of them among those having a wide applicability to various sectors and those that better could be implemented step-by-step by novice users. In particular, given a brief description of some commonly used risk identification methods (FTA, ETA, structured brainstorming, HAZOP/HAZID, matrices) that are among those strongly applicable to that initial step of the risk assessment, the book will focus on a barrier-based approach to risk analysis phase, discussing Bow-Tie, LOPA, RCA (via the BFA approach), HRA as single methods or in combination and applied to active and reactive phases of the RM cycle. Readers will notice that those have been judged to be among the best ways to be employed to fulfil the requirement of the risk analysis phase. At the end, some indications will be given for a cost-benefit assessment and consequence/probability matrix as methods to perform risk evaluation.

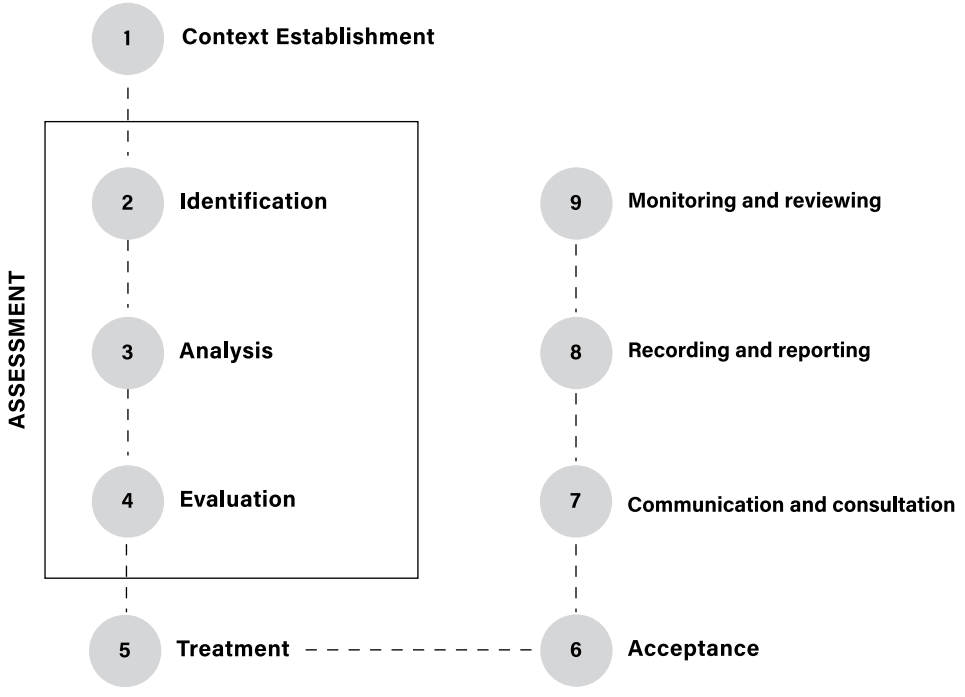


Figure 21 The risk assessment phase in the context of the RM process.

The risk assessment provides an understanding of the risks, their causes and consequences, and their probabilities (defined as the probability of the hazard as modified by present and planned measures). This provides important input to decide:

- If an activity must be performed;
- How to maximize opportunities for improvement;
- Which risks need to be treated, in order to reduce (possibly further) their level;
- How to prioritize risk treatment options;
- How to select the most appropriate risk treatment strategies capable of bringing high levels of risk to tolerable or acceptable levels, including in relation to the resources required (e.g. associated costs and time).

Risk assessment may often require a multidisciplinary approach, as the organization's risks can cover a wide range of causes and consequences and, as anticipated, combinations of risks and control measures often need to be considered.

This process should be properly documented and risks should be expressed in comprehensible terms so that the level of risk assessed is clearly communicated to stakeholders. Generally, the generated reporting should include at least the following information:

- Objectives and scope of work;
- Description of the relevant parts of the system and their functionality;
- Summary of the external and internal context of the organization and how it manages the system, the situation, or circumstance under assessment;

Table 1 Applicability of tools for risk assessment.

		Risk Assessment Process				
			Risk Analysis			
Tools and Techniques	**Paragraph**	**Risk Identification**	**Consequence**	**Probability**	**Level of Risk**	**Risk Evaluation**
Brainstorming	2.2	SA	NA	NA	NA	NA
Checklists	2.2	SA	NA	NA	NA	NA
HAZOP	2.2	SA	SA	A	A	A
RCA	3.5	NA	SA	SA	SA	SA
ETA	2.2	A	SA	A	A	NA
FTA	2.2	A	NA	SA	A	A
LOPA	2.14	A	SA	A	A	NA
HRA	A.3	SA	SA	SA	SA	A
Bow-Tie	2.3	NA	A	SA	SA	A
FN curves	2.2	A	SA	SA	A	SA
Risk indices	2.2	A	SA	SA	A	SA
Consequence/probability matrix	2.2	SA	SA	SA	SA	A
Cost/Benefit Analysis	2.2	A	SA	A	A	A
	SA = Strongly Applicable NA = Not Applicable A = Applicable					

Source: Adapted from IEC/ISO 31010, 2019.

- Applied risk criterion and its justification;
- Limitations, assumptions and justification of hypotheses and assumptions made;
- Methodology (or methodologies) chosen for the evaluation, reasons for the choice made, and degree of detail deemed necessary;
- Results of the hazard identification and consequent risks;
- Data used, their sources and validation;
- Results of the risk analysis and their evaluation;
- Sensitivity and uncertainty analysis;
- Discussion of the results;
- Conclusions and recommendations;
- Bibliographic references, with particular reference to the methodologies taken as reference and their applicability to the specific case.

1.3.8 Risk Identification

Each organization should identify the hazards associated with its processes, products and services, sources of risk, areas of impact, events (including context changes), their causes and potential consequences. The objective of this phase is to generate an exhaustive list of risks based on those events that could create, increase, prevent, accelerate, or delay the achievement of the objectives. It is also important to identify the risks associated with the failure to pursue opportunities for improvement, which will be discussed later in this book. A comprehensive identification of risks is essential, as a risk not identified at this stage will not be considered in the subsequent analysis.

The identification should include those risks whose source is or is not under the control of the organization, even when not immediately identifying their source or causes. Risk identification should include an examination of domino effects, identifying cascading and cumulative effects.

Each organization should apply the risk identification tools and techniques that best suit its objectives and capabilities, as well as the risks it faces. Relevant up-to-date information is important in identifying risks; therefore it is important to know the background information, where available.

Once the risk has been identified, the organization should identify any existing risk control measures put in place, whether related to design, behavioural aspects, or hardware or software processes and systems. Such control measures may be active or passive and in any case characterized by an intrinsic probability of failure in relation to the performance (degree of risk reduction) that they are supposed to operate.

Methods for risk identification include:

- Evidence-based methods, such as checklists and revisions of historical statistical data;
- Team approaches, where a team of experts follows a systematic process of risk identification by means of structured sets of questions or instructions;
- Inductive reasoning techniques, such as HAZOP.

Regardless of the technique used, at this stage it is also important to identify organizational and human factors. Therefore, deviations of human factors from what is expected must be included in the risk identification process in the same way as “hardware” or

"software" events. For this reason, this volume devotes a specific appendix to the topic. While human action can be the cause of a negative event, it is also a mode of response and intervention. Consequently, specific investigations must be carried out in order to understand both mechanisms.

1.3.9 Risk Analysis

Risk analysis is the phase in which the understanding of risk is developed. It provides input to the following phase of risk evaluation and enables a decision to be made as to which risks need further treatment in relation to the established acceptance criteria, as well as identifying the most appropriate strategies and methods for doing so. This phase can also provide input to the decision-making process of choosing between several treatment options covering different types and levels of risk.

Risk analysis consists of determining, by combining them, the consequences and associated probabilities of risk events identified in the previous phase of hazard identification, taking into account the presence – or absence – and the effectiveness of existing control measures. The level of consequences and their likelihood of occurrence are then combined to determine the level of risk (Figure 22), whose definition provided by ISO Guide 73 is: "Magnitude of a risk or combination of risks expressed in terms of the combination of consequences and their likelihood."

A risk analysis is based on the causes and sources of risk, their consequences, and the likelihood of these consequences occurring. Therefore, the factors influencing the level of severity of the consequences and their probability must necessarily be identified. It should be borne in mind that a single event can have multiple consequences and have an impact on several targets.

This phase normally includes an estimate of the severity of the consequences (effects) that may arise from an event, situation or circumstance, and their associated probability of occurrence, in order to measure the level of risk. However, sometimes in simple cases where the expected consequences are not significant and the associated probability of occurrence is estimated to be extremely low, a single parameter may be sufficient to make an estimate.

The methods used for risk analysis may be qualitative, semi-quantitative or quantitative. The degree of detail required will depend on the particular application, the availability of

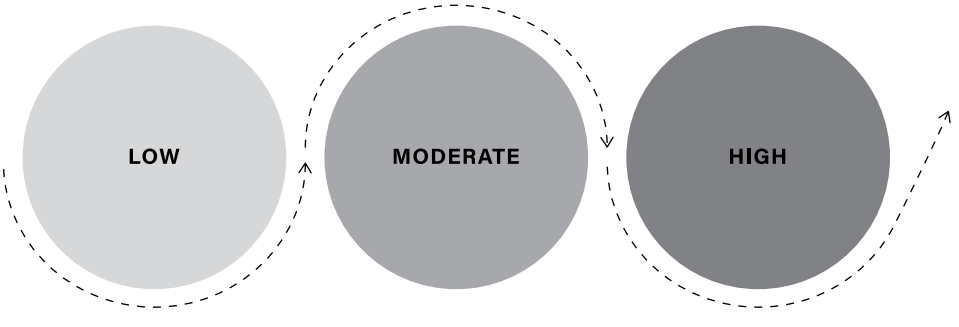


Figure 22 Level of risk.

reliable data, and the decision-making needs of the organization and of course the type of risk (and its potential effects). Some methods and the degree of detail of the analysis may be prescribed by a specific law with which the organization is obliged to comply.

Qualitative assessments define the consequences, the probability and the level of risk through levels of significance, such as high, medium, and low, thus assessing the resulting level of risk from the combination of consequences and probability through a qualitative criterion.

The semi-quantitative methods use numerical scales for consequences and probabilities and combine these levels to produce a level of risk by adopting a specific formula. The scales can be linear or logarithmic or have other types of relationships; the formulas used are the most varied.

The quantitative risk analysis (QRA) estimates, through numerical values often expressed according to codified parameters, including risk indices, the level of consequences and their probability, and produces values of the risk level in specific units defined in the previous phase of context identification. A quantitative risk analysis may not always be possible or desirable due to insufficient information on the system or activities analyzed, lack of data, complex influence of human factors, complexity and severity in terms of the extent of the complete survey, and so on. In fact, sometimes quantitative analysis is not applied because such an effort is not required and it is sufficient to adopt a semi-quantitative or qualitative analysis that is certainly synthetic but also immediately expendable and clearly effective.

In cases where qualitative analysis is used, it is good to provide a clear explanation of the terminology adopted and the reasoning behind the definition of the criteria used.

Even in cases where a quantitative risk analysis is adopted, it is good to keep in mind that calculated risk levels are always estimates. It must therefore be ensured that these risks are not attributed a level of accuracy and precision inconsistent with the accuracy of the data and methods used.

The results of this phase must be expressed in clear terms depending on the type of risk and in a form that provides easy input for the next phase of risk assessment.

1.3.10 Analysis of Control Barriers

Risk levels will depend on the adequacy and effectiveness of existing control measures. The analysis of control barriers requires that it highlight:

- The existing control measures for a specific risk;
- Whether these barriers are capable of dealing adequately with the risk so that it is managed at an acceptable level;
- Whether the control measures are operating as intended (as designed) and whether their effectiveness can be demonstrated (even over time).

The answers to these questions can only be provided with certainty if adequate documentation is available and if the way in which the processes under analysis are managed is well known, as well as the conditions under which the barriers can correctly reduce the risk assigned to them.

The level of effectiveness (or, using a synonym, of maturity) of a particular control measure can be expressed qualitatively, semi-quantitatively or quantitatively, according to the

type of analysis adopted. Although it is generally difficult to express a measure of effectiveness in a highly accurate manner, it is nevertheless useful to express and record a measure of the effectiveness of the control barrier in such a way that it is possible to make an informed judgement as to whether it is convenient to improve the performance of the same barrier or to adopt a different risk control measure.

1.3.11 Consequences Analysis

The consequences analysis, to be combined for the risk estimation with the assessment of the probability of occurrence, allows the determination of the nature and type of impact that could occur assuming that a particular event could happen. The same event may have different impacts of different magnitude, affect the fulfilment of different objectives of the organization, and influence different stakeholders. The types of consequences to be analyzed and the targets that are affected must be established at the context definition stage.

Consequence analysis can range from a simple description of the findings to detailed quantitative modelling.

Consequences may have a low level of impact but a high probability of occurrence, or vice versa (a high level of magnitude and a low probability of occurrence) or intermediate values. In some cases, it may be appropriate to focus on risks with very severe consequences, regardless of their probability of occurrence. In other cases, it may be equally important to analyze risks with low-level consequences but whose impact is frequent or even chronic with cumulative or not negligible long-term effects.

The analysis of consequences requires that:

- Existing control barriers are taken into account, together with all relevant factors that contribute to having an effect on the magnitude of the consequences (including, of course, any escalation factors).
- The consequences of the risk are always related to the objectives of the risk management system originally defined.
- Consequences relevant to the scope of the risk assessment are considered, i.e. those in line with the defined scope and work perimeter.
- Secondary consequences (so-called domino effects) are also considered, such as those affecting systems, activities, equipment or organizations connected to the risk assessment scope, also taking into account the common causes of failure and the impact on critical systems and processes for the organization.

1.3.12 Frequency Analysis and Probability Estimation

Probability estimation is generally performed according to three approaches (Figure 23) that can be used individually or jointly:

1) Use of reliable and relevant historical data to identify those events that occurred in the past from which it is possible to extrapolate their probability of occurrence in the future. The data used must be relevant to the type of system, organization and activity considered. If the historical analysis reveals a very low frequency of occurrence, then any estimate of probability that can be derived from it will be affected by great uncertainty. This

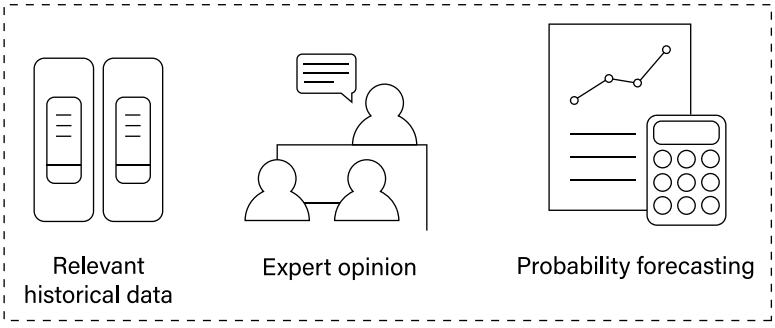


Figure 23 Frequency analysis and probability estimation.

is particularly true when there are no historical events of the type being investigated, so it cannot be concluded that such an event (or circumstance) will not occur in the future.

2) Use of predictive techniques such as the fault tree or event tree, which will be discussed more extensively in the next chapter. When historical data are not available or are not adequate, it is necessary to derive the probability from the analysis of the system, activity, equipment or organization, noting their states of success or failure. The numerical data are then combined to produce an estimation of the probability of occurrence of the adverse event under consideration. When using techniques of this type, it is important to ensure that the analysis is carried out with the right expertise, as common causes of failure on different parts or components of the system leading to the same cause may be found. Sometimes, some simulation techniques can be used to generate the probability that an equipment will fail due to ageing and degradation processes, taking due account of the effects of uncertainties.
3) Expert judgement used in a systematic and structured way for the estimation of probabilities. This approach has been formalized by a number of methodologies, some of which are also set out in ISO/IEC 31010.

1.3.13 Preliminary Analysis

It is important to identify the most relevant risks and exclude from the subsequent analysis phases those that are less significant in relation to the context, the complexity of the organization and the defined objectives. The objective is to ensure that resources are prioritized to the most significant risks for the organization. In doing so, due attention must be paid to low impact and high frequency risks that can have significant domino, cumulative, and long-term effects.

The selection of the "most significant" risks should be based on criteria defined in the previous context definition phase. The preliminary analysis determines the course of the following actions:

- Decide to treat the risks without further evaluation;
- Set aside those non-significant risks on which treatment would not be justified (also economically, according to an ALARP (as slow as reasonably practicable) approach);
- Proceed with a more detailed risk assessment in order to have more information for decision-making.

1.3.14 Uncertainty and Sensitivity of the Analysis

Risk analysis is often affected by a non-negligible degree of uncertainty. Understanding this uncertainty is necessary to interpret and communicate the results of risk analysis effectively. The analysis of uncertainties associated with data, methods and models used to identify and analyze risk plays an important role in their application. Uncertainty analysis involves determining the variability or inaccuracy of results as a outcome of the collective variation of the parameters and assumptions used to define the results. An analysis similar to that of uncertainties is the so-called sensitivity analysis.

Sensitivity analysis first of all must allow the determination of how the level of magnitude of the consequences of the risks changes as the input parameters vary. It can be used to identify those data that must necessarily be accurate and those that are less sensitive for which high accuracy is therefore not required.

The sources of uncertainty of the parameters that govern risk analysis with greater sensitivity must be adequately stated and communicated to all stakeholders, including, first and foremost, those involved in the assessment process.

1.3.15 Risk Evaluation

The objective of the risk evaluation is to assist the organization in the decision-making process, based on the results of the risk analysis, about which risks need to be treated, as well as identifying the priorities for the implementation of such treatment.

The risk evaluation is carried out by comparing the risk levels estimated in the previous phase of the analysis with thresholds of acceptability (or tolerability) defined by a pre-established criterion. Based on this comparison, the need for further action to reduce the level of risk is analyzed. These decisions should take into account the assumptions and models on the basis of which the previous phase of analysis was carried out, in order to properly consider the tolerances and sensitivities of the data obtained. Such decisions should also be made in accordance with legal requirements where defined.

Possible decisions include the following:

- Whether a risk must be subjected to the next stage of treatment;
- Set priorities for treatment;
- Which of the possible alternative solutions to achieve the desired result should be followed, as well as in relation to the resources that need to be employed.

Sometimes the risk evaluation may lead to the decision to undertake further in-depth risk analysis studies; other times it may lead to the decision to maintain existing control barriers, thus accepting the pre-existing level of risk. These decisions are influenced by the company's risk appetite and the criteria of acceptability and tolerability that the company has set when setting its objectives, in accordance with the risk management policy.

1.3.16 Acceptability and Tolerability Criteria of the Risk

The simplest approach to defining a risk acceptability and tolerability criterion is to divide risks into two categories: those requiring treatment and those not requiring treatment. This

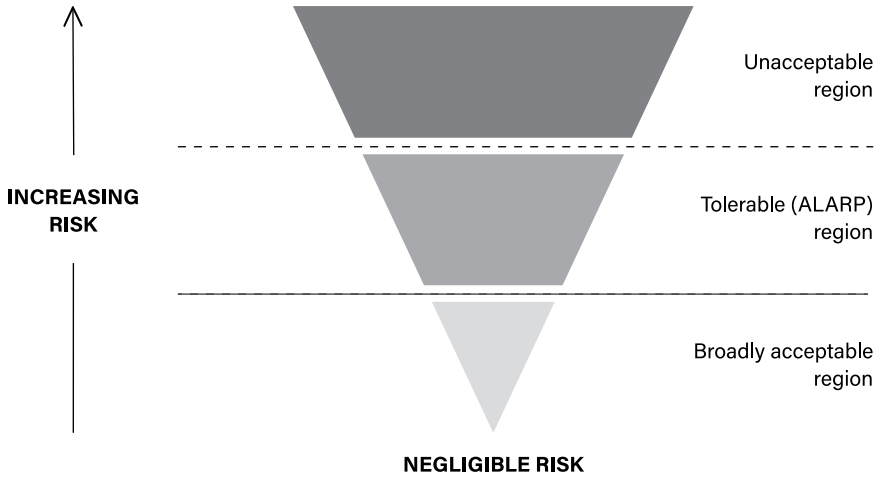


Figure 24 Risk acceptability and tolerability thresholds.

approach leads to seemingly simple results, but it does not reflect the uncertainties inherent in estimating risks and defining the boundary between risks that will need to be treated and those that will not. Once it is clarified that the risk acceptability and tolerability criterion must be defined by the organization on the basis of its own principles and risk sensitivity, the decision whether or not to treat a risk may depend on the costs and benefits of implementing any additional control measures. For this reason, a cross-sectoral approach across various industries is to divide risks into three bands (Figure 24):

- A higher band, where the level of risk is considered intolerable whatever the benefit of the risky activity. In this band, the treatment of the risk is essential, whatever the cost;
- An intermediate band, where the relationship between the costs and benefits expected from the implementation of additional measures is considered, comparing opportunities and potential consequences;
- A lower range, where the level of risk is considered acceptable, or such that no further treatment is required.

One of the most common methods for the representation of the risk acceptability and tolerability ranges is the risk matrix, within which reference ranges based on effect categories and/or probability classes can be identified.

1.3.17 The Risk Matrix

The risk matrix is a useful tool for the graphical visualization of risks and the combination of their magnitude and frequency levels (Figure 25). It is particularly used when a semi-quantitative analysis is carried out. This type of analysis, as already discussed, uses a numerical approach, typical of a quantitative analysis, together with simplifying and conservative assumptions about the evaluation of the level of severity of consequences, the evaluation of the frequency of occurrence of the initiating causes of an event, and the efficiency of control measures. Generally, the results of a semi-quantitative analysis are

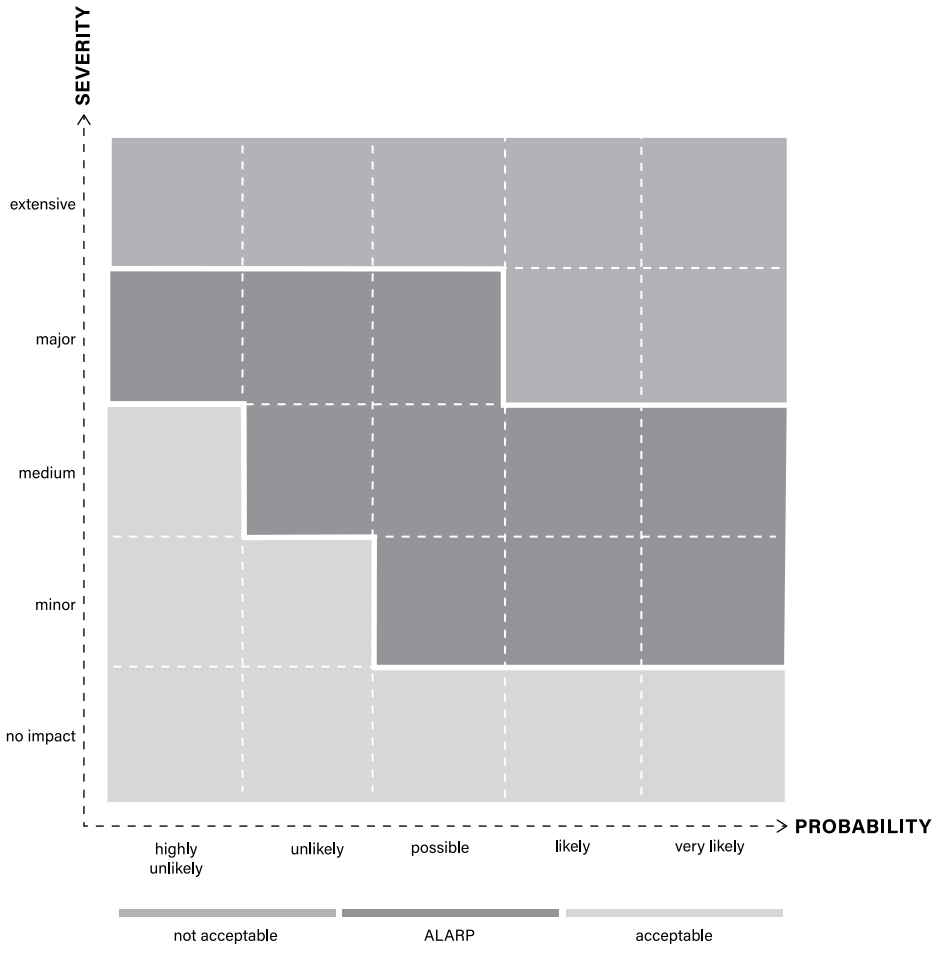


Figure 25 Example of a risk matrix with level of acceptability regions.

expressed in orders of magnitude. However, a risk matrix is also generally used for qualitative analysis, such as that in Figure 25. In it, both probability and severity are expressed in qualitative terms, which must be evaluated by an experienced team to assign the appropriate level of risk, given by the combination of a given severity class with a specific probability class. On the other hand, in a semi-quantitative analysis, the frequency of occurrence is generally expressed on occasions per year (occ/year) while the consequences are identified through a progressive level from 1 (the least severe) to 5 (the most severe), in relation to the severity of the expected consequence. In the example, the grey region defines the most severe risks. A risk falling in this region often requires the immediate stop of the organization's activity in this area, being absolutely unacceptable. The blue area of the matrix identifies a particular region of the matrix where the risk could be accepted (tolerable risk). The risks in this region require an ALARP study. Briefly, this is a cost-benefit analysis of the potential intervention required to further mitigate the risk in order to target the region of acceptability. Since mitigation may require an economic effort that is not justified by the

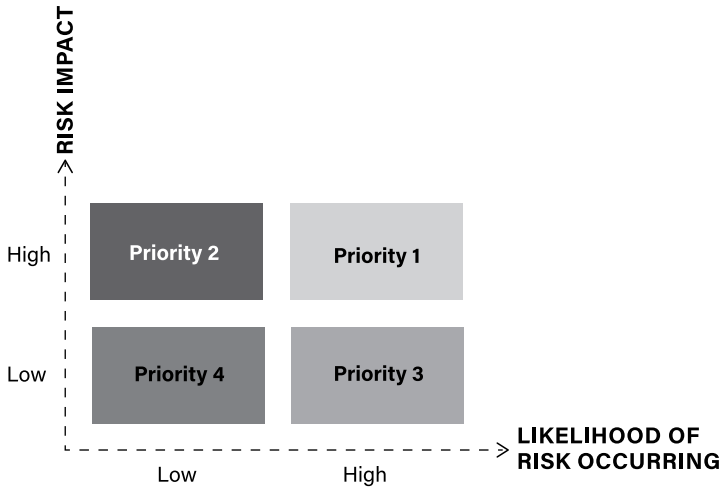


Figure 26 Prioritization of risk given impact and liklihood.

reduction of the level of risk, a risk falling within the ALARP region could be accepted as such: the managers (or, in general, whoever is responsible for the risk) will take responsibility for this choice based on a cost-benefit analysis.

Finally, the green region is about acceptable risks: no further ALARP mitigation or study is required for them.

ALARP is not the only risk acceptance criterion available. There are also other criteria, such as GAMAB (globally at least as good), MEM (minimum endogenous mortality), MGS (at least the same level of safety), NMAU (not more than unavoidable), but it is not the subject of this book to address them, so the ALARP study, one of the most widespread in the world of risk management, will be considered.

The graphic representation of the risk level through the matrix allows the introduction of the risk prioritization (Figure 26), i.e. the possibility of assigning a degree of priority to the various risk treatment options that will be offered, as better explained shortly.

The prioritization of risk allows the organization to make risk-based decisions, thus allowing itself to be guided in decision-making processes by the need to target an acceptable level of risk. In the case of the risk matrix shown in Figure 27, this means prioritising scenarios with a risk level close to the top right (very high impact). The proposed graphic representation guarantees a good communication of information to all stakeholders, while pursuing the principle of inclusiveness of risk management.

1.3.18 The ALARP Study

Each organization should support ALARP studies, helping to develop a comprehensive risk mitigation strategy for scenarios deemed credible, identifying and prioritising any viable risk mitigation action that can reduce the risk associated with a scenario up to an ALARP level. In addition, for those scenarios without the opportunity to further reduce the level of risk, each organization should provide a mechanism to document that the risk considered is already at a tolerable level (ALARP).

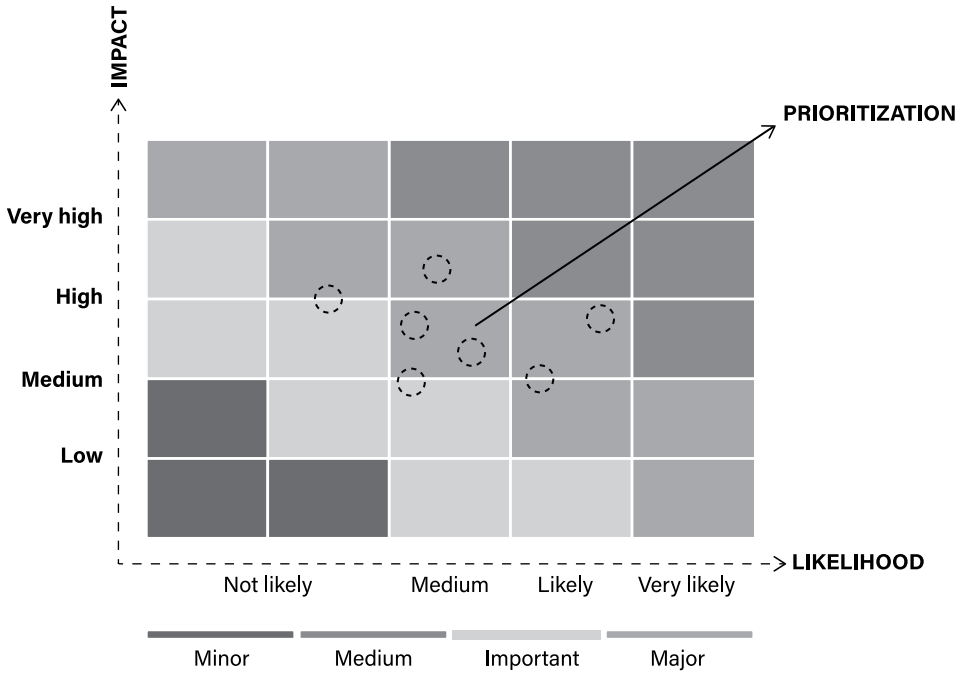


Figure 27 Risk prioritization and the risk matrix.

ALARP studies should be undertaken using a documented process and performed by personnel familiar with the details of the risk scenario being assessed. Typically, the personnel dedicated to ALARP studies are the same personnel who carry out the risk analyses.

Any potential risk mitigation opportunities identified within the ALARP process will be documented as follows:

- A recommendation;
- An option that is not recommended because of its impracticability in relation to the resources to be put in place (including those for maintaining the recommendation over time);
- An option that is not recommended because of other identified and deemed more favourable risk mitigation opportunities.

It should be noted that risk mitigation alternatives are often not mutually exclusive, so multiple recommendations could result from the ALARP study of a single risk scenario. Moreover, not all risk mitigation measures or recommendations in an ALARP study will generally be classified as control measures (barriers). Those recommended actions that cannot qualify as barriers, because they do not produce a reduction in the risk level by acting on the frequency of occurrence or severity of a scenario, will be collectively identified as "other measures." Examples of "other measures" could be – depending on the specific context – warning signs or labelling. "Other measures" are typically identified as actions to be applied to consequences whose risk is already acceptable.

An ALARP study aims to answer the following questions in a structured way, for each risk scenario assessed:

- What alternatives are available to eliminate, reduce or manage the risk?
- What factors determine the feasibility of any risk mitigation alternatives?
  - How much risk mitigation is substantially achieved by the measure?
  - What resources are needed to implement the measure?
  - What synergies would be achieved if the measure is implemented?
  - Should the measure also be implemented in similar facilities/workstations?
  - Is the measure congruent with the current practices adopted in the reference work sector?
  - What is the technical and operational feasibility of the measure?
  - How long would the implementation of the measure take?
  - What other risks would be impacted by the implementation of the same measure?
  - What is the availability of the measure?

In general, the risk reduction strategy imposes a hierarchy of possible options in the following order:

- Eliminate the hazard (e.g. by changing the activity, process, system under consideration and source of the risk considered).
- Reduce the hazard (e.g. by reducing the amount of flammable substances stored in the warehouse).
- Control the hazard through additional measures (barriers).

According to this hierarchy, for example, an action that eliminates the hazard will have a much greater benefit than the installation of an additional barrier to control it.

Before carrying out an ALARP study, an organization might ask itself whether the action required to reduce a specific risk has already been taken with positive feedback from other assets in the same organization or from other competitors. It is also necessary to ask first of all whether the suggested action is in fact a requirement arising from new mandatory regulations or standards or international best practice. In such cases, the organization may decide not to carry out any cost-benefit analysis, deciding a priori to implement the new measure.

Although there are different methodologies to perform a cost-benefit analysis, for the purposes of this book it seems sufficient to mention qualitative analysis.

It is based on the adoption of a matrix like the one in Figure 28. For each risk falling within the risk tolerability region (i.e. the ALARP region of the risk matrix in Figure 25), the analyst considers the costs (e.g. in financial and/or time terms) and benefits (in terms

		Expected benefits		
		High	Average	Low
Associated costs	High			
	Average			
	Low			

Figure 28 Matrix example for qualitative ALARP analysis.

of risk reduction) expected from the implementation of a particular option. The scale of benefits could for example be as follows:

- High: The risk leaves the ALARP region and becomes acceptable.
- Medium: The risk reduces in level, but remains in the ALARP region of risk tolerability.
- Low: The measure does not reduce the level of risk.

The definition of the cost level will typically depend on the sensitivity of the organization and other strategic policy criteria, both in economic-financial and temporal terms. According to the example matrix in Figure 28, high-cost and low-benefit options will not be implemented, while high-benefit measures will always be implemented, regardless of the costs associated with their implementation.

When calculating associated costs, it is necessary to consider both the resources required for the design of the further control and those connected with its implementation and maintenance over time. It is also useful to consider not only direct costs for implementation and operation but also indirect costs (inspection, testing, and periodic maintenance or information and training for use). In fact, like the risks they intend to reduce, the controls have their own life cycle, within which the resources for maintaining efficiency over time could play a crucial role and be a discriminating factor in the selection of the most appropriate treatment measure.

In conclusion, the objective of the ALARP study is therefore to offer a cost/benefit assessment, which can be summarized in Figure 29.

1.3.19 Risk Management over Time

Risk management does not end with a snapshot taken at a certain moment, but instead requires a dynamic approach. This is done first by following the risk assessment phase with the treatment phase. The risks analyzed will in any case be monitored and reviewed; as additionally, the entire structured approach to risk management (the framework) will be monitored and reviewed at predetermined intervals, thus reviewing the performance of the system.

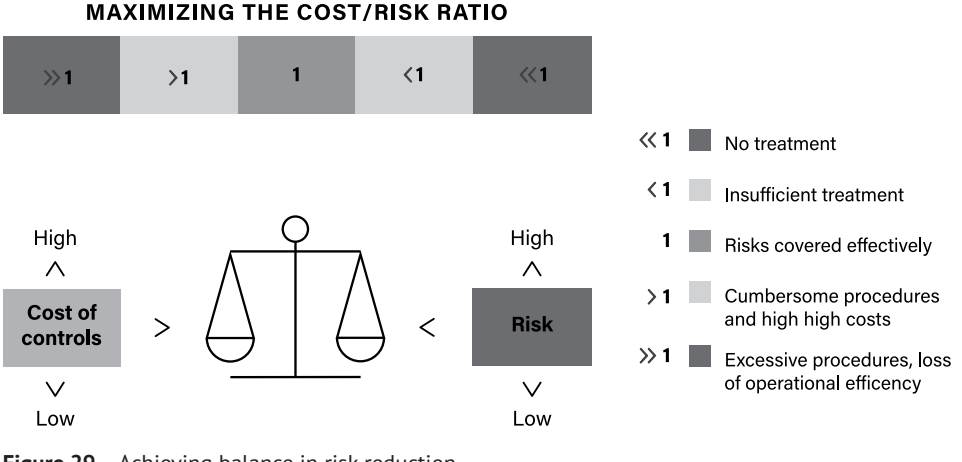


Figure 29 Achieving balance in risk reduction.

1.3.20 Risk Treatment

The risk treatment often requires the choice of one or more options to modify the risks assessed during the previous evaluation phase and then implementing these options. Once implemented, the risk treatment generally provides new control measures or changes to existing ones. This is a cyclical process consisting of the following steps:

- Assessment of risk treatment;
- Decision whether the residual risk, i.e. the level of risk obtained downstream of the implementation of the treatment, is tolerable;
- If the level of risk is not tolerable, generate a new risk treatment;
- Assess the effectiveness of this new treatment.

As discussed above, risk treatment options are not necessarily mutually exclusive or suitable for all circumstances. Generally, the possible options are as follows:

- Avoid risk by deciding not to start or continue the risky activity.
- Remove the source of the risk.
- Change the frequency of occurrence of the damaging event, with interventions aimed at reducing the frequency of its causes or reducing the probability of failure on demand of control measures.
- Change the level of expected consequences, for example by increasing the effectiveness of mitigating control measures.
- Share information on the risk level with other parties, including contractors and insurers.
- Accept the risk through an informed and aware decision.

Selecting the most appropriate risk treatment option often involves a cost-benefit analysis, already mentioned in the ALARP study previously introduced, always bearing in mind the legal requirements, the social responsibility, and the environmental protection. Each organization should also make decisions on risks that may require treatment that cannot be justified on economic basis, such as risks with very severe yet extremely rare consequences.

When choosing risk treatment options, the organization should consider the values and perceptions of stakeholders, who should be involved in the decision-making process, by adopting the most appropriate means of communication with them. Indeed, although equally effective, some actions may be more easily accepted by some stakeholders than others.

The corrective action plan should clearly identify the priorities in risk treatment. It should be noted that the risk treatment phase may itself introduce new risks, such as the failure or ineffectiveness of the treatment measures chosen. If new secondary risks are introduced during the risk treatment phase and need to be assessed, treated, monitored and reviewed, then these risks should be incorporated into the same treatment plan as the "original" risks, avoiding treating them with a different process.

The objective of risk treatment plans is to document the treatment options chosen, clarifying how they are implemented. At least the following information should be contained in a risk treatment plan:

- The reasons for selecting a particular treatment option, including the expected benefits of such implementation;
- Who is responsible for approving the plan and who is responsible for its implementation;

- The proposed actions;
- The required resources (both instrumental and organizational-managerial);
- The performance measures and any constraints;
- The monitoring and documentation requirements (including the recording of evidence);
- The scheduling of actions according to a pre-established plan and based on the established priority.

Treatment plans (and not just the individual options contained therein) should also be integrated with the organization's management processes and discussed with all stakeholders.

Decision-makers and other stakeholders should be aware of the nature of the residual risk after the treatment phase; therefore, the residual risk should be documented and subject to monitoring and review and, where appropriate, further treatment. The risk treatment activities are summarized in Figure 30.

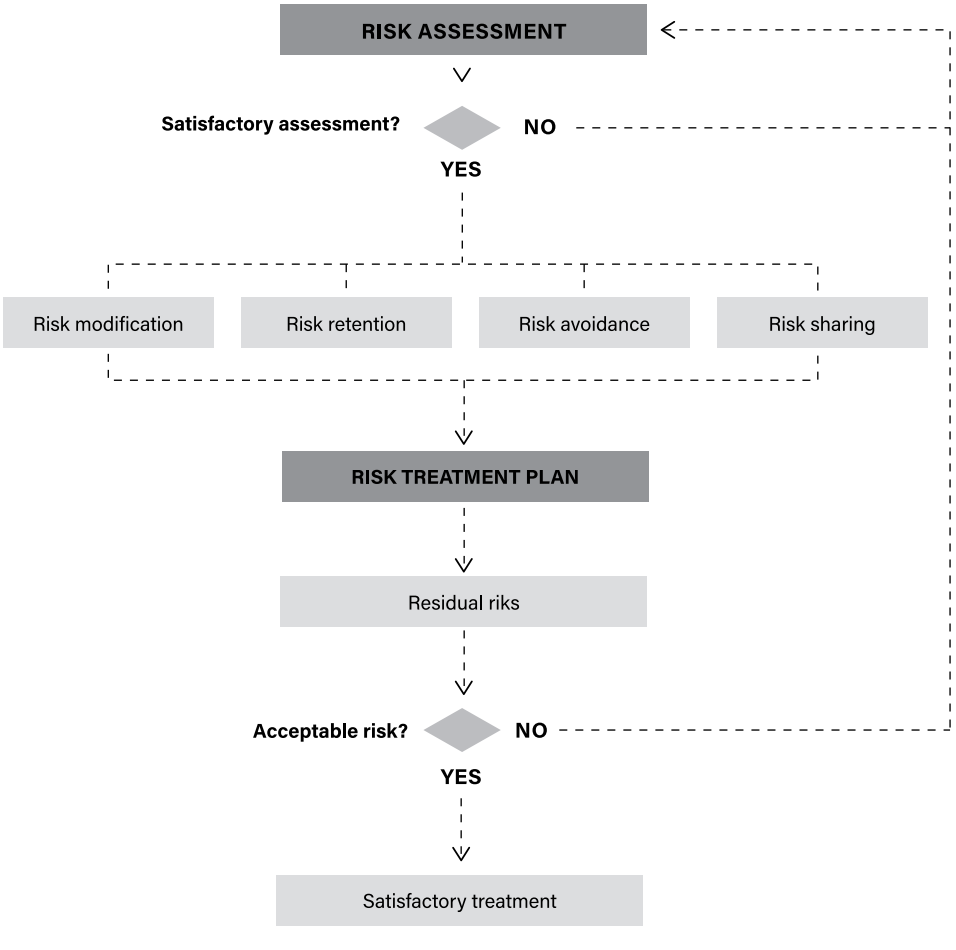


Figure 30 Risk treatment activities.

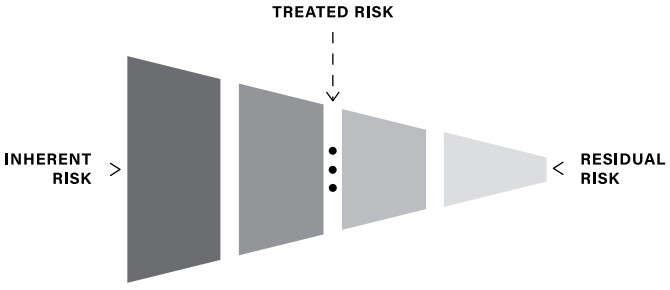


Figure 31 Residual risk.

At the end of the treatment phase, the inherent risk is reduced to a lower level, named "residual risk" (Figure 31). Residual risk can be defined as the risk that remains after the implementation of controls aiming to reduce the inherent risk.

1.3.21 Monitoring and Review

Both monitoring and review (also known as periodic review) are phases of the risk management process that involve, on a periodic or ad hoc predetermined basis, the verification and surveillance of the risks identified, analyzed, evaluated and treated and the related control measures. The persons responsible for the monitoring and review phases must be clearly identified within the organization. These phases should cover all aspects of the risk management process with the aim of:

- Ensuring that control measures are effective and efficient, both in design and operation;
- Obtaining further information to improve risk assessment;
- Analysing and learning lessons for improvement from events (including near-misses and anomalies), changes, trends, successes and failures;
- Identifying changes in the internal and external environment, including changes to the risk acceptability and tolerability criteria and the risks themselves that may require a review of corrective actions and related priorities;
- Identifying emerging risks, including in relation to the results of in-depth analysis of the root causes of adverse events.

The progress of the implementation of risk treatment plans provides a measure of performance to be monitored. The results can be incorporated into the management performance of the entire organization, internal and external documentation, and reporting measures and activities.

The results of the monitoring and review phases should be recorded and documented externally and internally when appropriate and should be used as input data for the review of the entire organizational risk management structure. This is in order to ensure that current risk management processes are commensurate with the size and complexity of the company as well as suitable for the defined objectives are maintained over time.

In general, all risk management activities should be traceable. In the risk management process, data and evidence are the basis for improving methods and tools, as well as the entire process. The decision to retain this data must take into account:

- The organization's needs for continuous learning;
- The benefits of reusing information for management purposes;
- The costs and benefits of creating and maintaining data records;
- Legal and operational requirements for data logging;
- How to access, retrieve and store multimedia data;
- The period of retention;
- The sensitivity of the information.

This includes periodic audit activities. The monitoring of systems through inspection (internal, second- or third-party inspection) guarantees the effectiveness and efficiency of the system.

1.3.22 Audit Activities

Regardless of whether third-party audits are applicable to the specific business context, the organization intending to adopt a risk management system must conduct, at planned intervals, internal audits in order to receive information useful to verify whether the risk management system is:

- Compliant with the organization's own requirements, including the risk management policy and the established objectives of the risk management system;
- Compliant with the requirements of ISO 31000 if selected risk management paradigm;
- Effectively implemented and maintained also in relation to changes that have occurred.

To verify this, the organization must:

- Plan, establish, implement and maintain one or more internal audit programmes, where frequencies, methods, responsibilities, consultation, planning and reporting requirements are clearly identified, taking into account the importance of the processes involved and the results of previous audits.
- Define the audit criteria and their scope.
- Select auditors and conduct audits ensuring objectivity and impartiality of the inspection process.
- Ensure that the results of audits are reported to relevant individuals such as managers, workers, and, if any, workers' representatives.
- Take action to address non-conformities arising from audits, thereby continuously improving the performance of the risk management system.
- Maintain documented information containing the results of audits and the implementation of the audit programme.

The interested reader can refer to the ISO 19011 technical standard which defines guidelines for management systems audits, where the competence required of auditors is also specified.

1.3.23 The System Performance Review

Not only must the specific risk management process be subject to periodic monitoring and review, but the entire corporate framework that supports these processes is also subject to review. The structured approach to risk management, in order to be effective and provide constant support in achieving company performance, must be monitored and reviewed. In this sense, the organization should:

- Measure the performance achieved in risk management through appropriate indicators, the appropriateness of which is periodically reviewed.
- Measure progress and deviations from expected targets on a regular basis.
- Periodically review whether the structure, policy and expected objectives are always appropriately defined, taking into account the external and internal context of the organization and related changes.
- Document risk, progress against expected objectives, and how effectively the risk management policy is implemented.

On the basis of the results of the monitoring and any revisions, the organisation is asked to express its opinion on any decisions to improve the framework, the policy, and the expected objectives in terms of risk management. Such decisions should lead to tangible improvements in terms of risk management culture and, overall, to the effective and efficient implementation of this organizational model, with small but certain steps, to fulfil the organization's policy and objectives (Figure 32).

The various technical regulations on management systems in any area identify this phase as a "management review." In this phase, senior management is required to periodically review the management system adopted. In doing so, it must also take into account:

- Status of actions resulting from previous reviews;
- Changes in internal or external context factors relevant to the management system, such as changed needs and expectations of stakeholders, change in legal requirements, or change in business risks;
- Level of implementation of the policy and objectives of the risk management system;

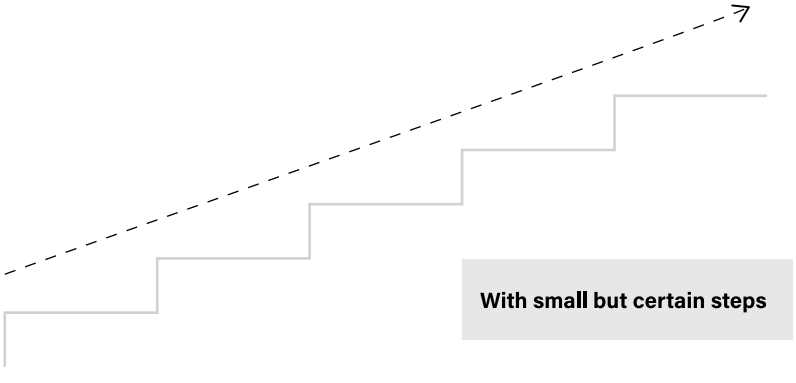


Figure 32 Risk management process continuous improvement.

- Information on the performance of the risk management system, including from the results of monitoring and measurement of performance standards;
- Adequacy of resources for the effective maintenance of the risk management system;
- Relevant communications with all stakeholders;
- Opportunities for the pursuit of the continuous improvement paradigm.

Appropriate documentation must be kept as evidence of the results of management reviews.

In order to make the overall review phase of the system more objective and structured, it is useful to define numerical indicators and monitor each process under review, from which trends and the achievement of the set objectives can be inferred.

At the end of the process, the risks need to be documented in a report (Figure 33), whose content should contain the information recommended by ISO 31000, whose format is consistent (date of emission, version number, author clearly identified, date of approval, and so on), and whose life cycle is properly managed.

The conclusion to this paragraph is dedicated to the person who is in charge with the risk management activities: the risk manager. Managing risk is a complex task and a risk manager should be appointed to ensure the required coordination. In this role, he/she should possess the following set of skills and knowledge, as identified in Figure 34:

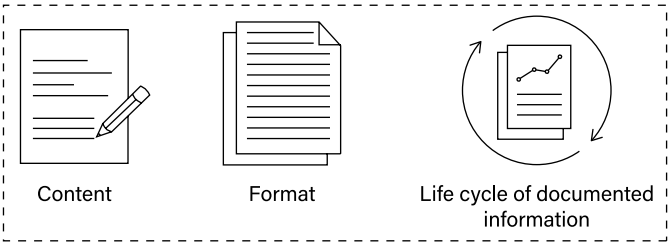


Figure 33 Documenting the risk management process.

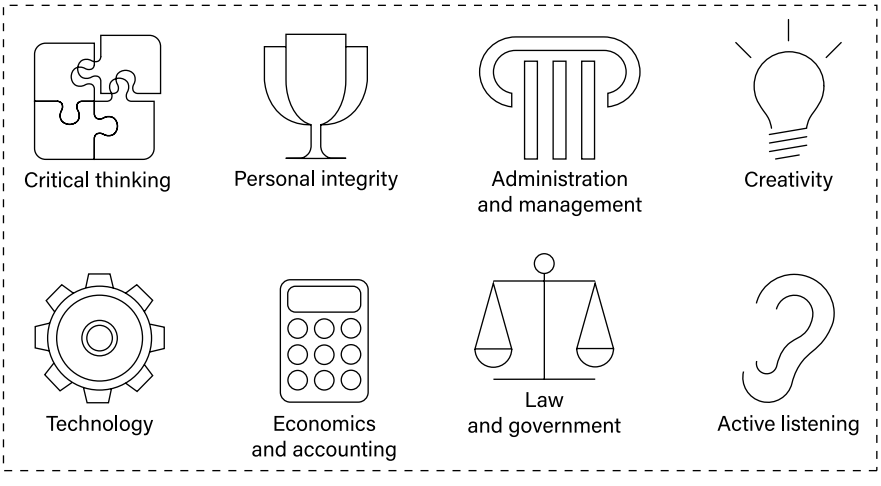


Figure 34 Skills and knowledge for a risk manager.

- Being a critical thinker, remaining logical and reasonable when identifying hazards, assessing risks, proposing solutions, or analyzing threats;
- Personal integrity, with a high level of morale;
- Being knowledgeable about administration and management;
- Being creative to finding smart solutions to challenging problems;
- Being knowledgeable and self-confident with technology;
- Being knowledgeable in finance and economics;
- Being knowledgeable in laws and politics;
- Being an active listener, ready to catch the opportunities coming from the comparison and the dialogue

In doing their job, regardless of the adopted work styles, risk managers should not make the mistake of feeling that they are solely responsible for managing the process. They are certainly the leader, but the proper implementation of the risk management system requires proper training of RM team members, a proper understanding of their responsibilities, and the creation of a sound infrastructure, which can be achieved only allocating the required resources (Figure 35).

A good risk manager ensures the strategic alignment between the RM objectives and the organization's goals (Figure 36). The consequent high level of consistency can be achived only through a deep understanding of the mission, objectives, values, and strategies of the organization.

At the end of this paragraph it is therefore worth highlighting how risk management is synonymous, in practical cases of risk treatment, with "risk control." Such risk control must follow the hierarchy and workflow that are summarized in Figure 37.

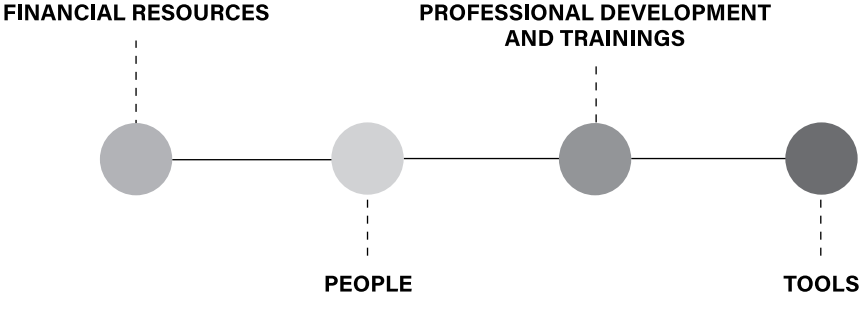


Figure 35 Resources to be allocated for an effective RM.

Figure 36 Understand the mission, objectives, values, and strategies.

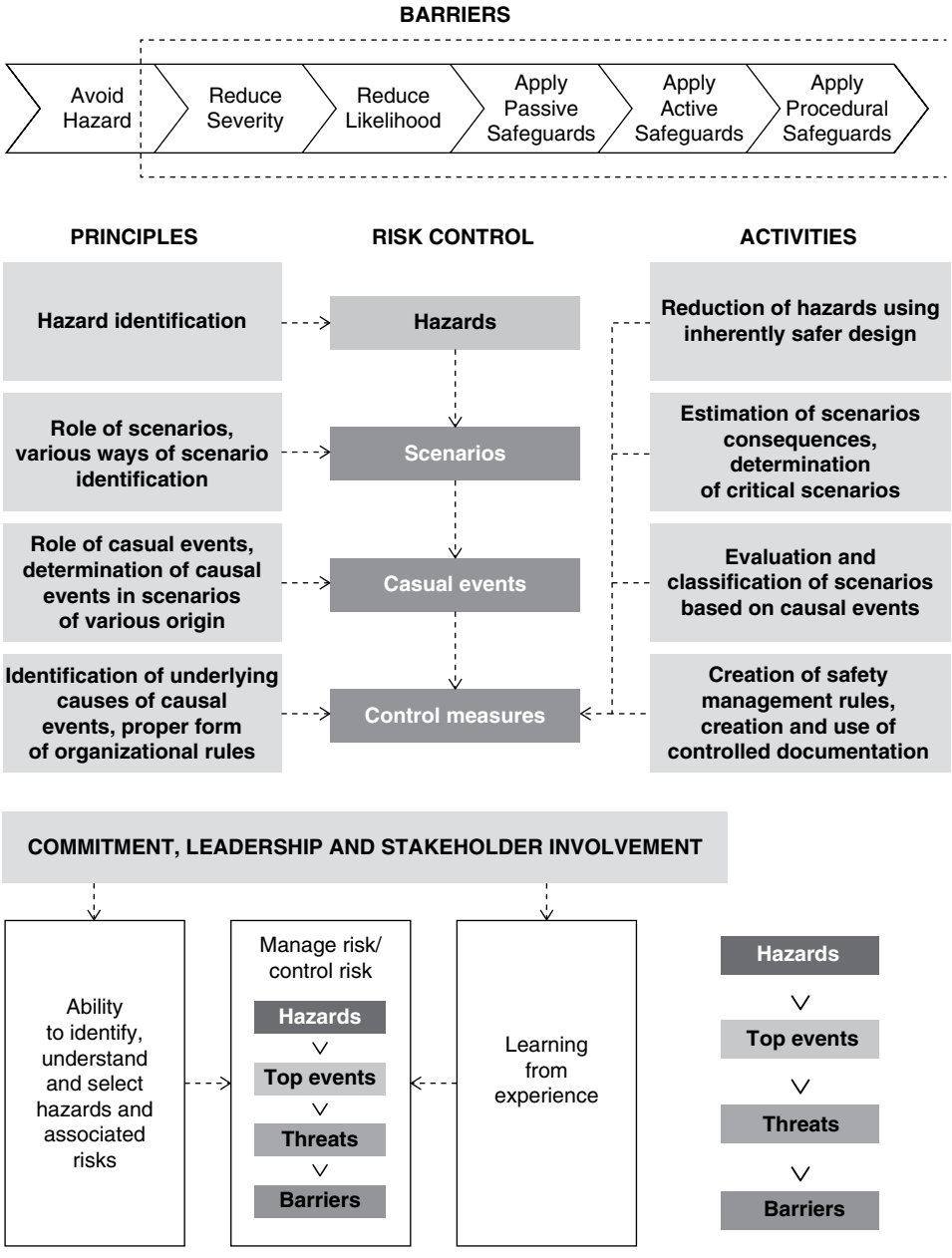


Figure 37 Risk control hierarchy and in practice.

From this perspective we observe Haddon's 10 strategies to control risks (Haddon, 1980): Pre-event

- Prevent the existence of the agent.
- Prevent the release of the agent.
- Separate the agent from the host.
- Provide protection for the host.

Event

- Minimize the amount of agent present.
- Control the pattern of release of the agent to minimize damage.
- Control the interaction between the agent and host to minimize damage.
- Increase the resilience of the host.

Post-event

- Provide a rapid treatment response for the host.
- Provide treatment and rehabilitation for the host.

1.4 Uncertainty and the Human Factor

The analysis of the human factor in risk assessment and incident analysis activities is fundamental to fully understand the impacts it can have on the organization, regardless of its type, scale, size and complexity or the role it played in real events or near-misses.

This chapter does not intend to provide a definitive description of the human factor (including human error), a subject for which numerous technical-scientific and popular publications are available at the international level, given the extent of all the topics related to this aspect and the ever-growing research in this field by institutes, researchers, experts, and consultants, as well as organizations, in the intimate discovery of their business processes. However, in the formulation of a risk assessment and a systemic approach to risk management, the study (qualitative or quantitative) of the human factor plays a fundamental role. This emerges powerfully by adopting a barrier-based approach for which, using intuitive graphical notations such as those proposed by methods like the Bow-Tie and barrier failure Analysis (BFA), the human factor is immediately recognized in some causes of risk, in the vulnerability associated with impacts and also in control measures (barriers constituted by the human response, barriers that do not guarantee their performance for aspects related to information, skills, or training, or fail totally due to human errors in the conduct of technical activities such as periodic maintenance on critical technical systems).

Often, human errors are recognized as the root cause of an accident, near-accident or non-conformities (including process anomalies), losing the opportunity for the organization to initiate an introspective analysis to find out how fertile ground could be provided for people, whose activity is part of a wider organizational structure, to make a mistake. Even tracing a cause back to the generic "human error" without further evaluation or investigation is absolutely reductive, if not totally useless. The failure to take into account human factors with an awareness of the point within the risk management and incident analysis activities, both provided for by ISO 31000, does not therefore allow the organization to follow up an effective plan of actions aimed at preventing the recurrence of similar events, thus denying itself the opportunity to pursue the rationale of continuous improvement. In order to do this, it is necessary to identify and evaluate certain performance factors, including ergonomics, workload, training, degree of competence and training, work organization and others.

It is therefore important to recognize, through examples collected from experience, the precursors of human error, identifying possible measures for their prevention that should be included in the risk analysis, and taking advantage of the barrier-based perspective increasingly established internationally.

The integration of human factors within risk management also requires that models and methods for the quantification of the probability of error are available, represented every day by methods such as THERP, HEART, SPAR-H and many others.

In the process industry sector, many authors have collected experiences and examples of human error within entire volumes. This is the case of Strobhar (2013), Woods et al. (2010) and Taylor (2016).

This chapter therefore aims to provide the basic knowledge to address the issue of human factors within organizations that intend to incorporate these aspects within the broader risk management according to the ISO 31000 standard (including other voluntary standards which, sharing the same structure, provide for the conduct of risk assessments, such as ISO 9001, ISO 14001, and ISO 45001) which, in context analysis, also explicitly requires the human factor to be considered.

The handling of such a complex topic is based on the knowledge of the main models of human information processing, together with the knowledge of behavioural patterns.

According to one of the most widespread human behavioural models (Forck and Noakes Fry, 2016), values and everything in which an individual believes (i.e. his opinions and faith) influence his or her way of reasoning and therefore his or her thoughts. These, in turn, influence the individual's behaviour, i.e. the way he or she acts. Behaviors can therefore lead to results, including an accident, near-accident or non-conformities. In order to modify the behaviour of individuals it is therefore necessary to change their mental model, their beliefs, and their values, as shown in Figure 38. It is hence necessary to act on the invisible in order to have results on the visible level.

It is then clear that the behaviour of an individual is peculiar to the individual him/herself with respect to a common stimulus (although, if we go deeper we can also say that the

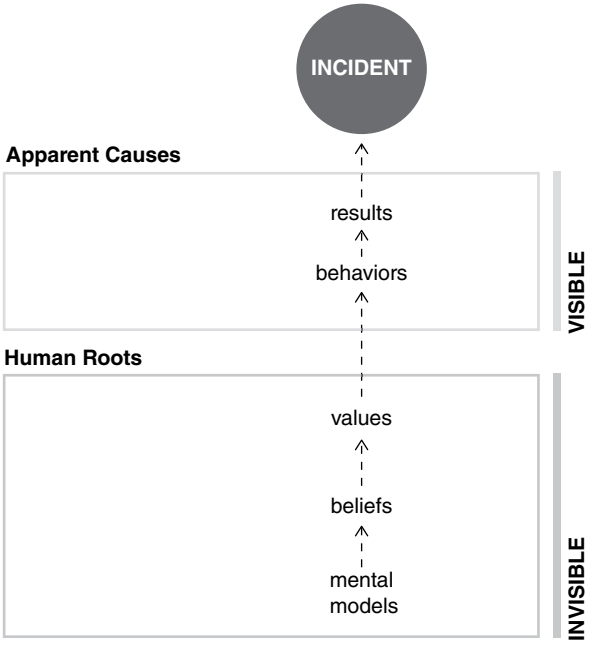


Figure 38 Thinking-Behavior-Result model. *Source:* Adapted from Fiorentini and Marmo (2018).

individual behaviour can be modified by the observation of the overall behaviour of a multitude of individuals, e.g. in the response of a mass of people in case of evacuation).

According to another model (Forck and Noakes Fry, 2016), the mental process is activated by a stimulus, which produces a response, i.e. it shapes human behaviour. The result is the consequence. In the incident analysis, the model is reversed as shown in Figure 39. Therefore, first the result (the accident) is analyzed by identifying what happened. Then, the analysis of the response clarifies how it happened. Finally, by reconstructing the mental process, it is possible to evaluate the stimulus that activated the sequence, thus establishing why the accident happened.

According to a third model (Forck and Noakes Fry, 2016), the success of human performance is achieved when certain internal and external factors affecting human abilities are met, as shown in Figure 40.

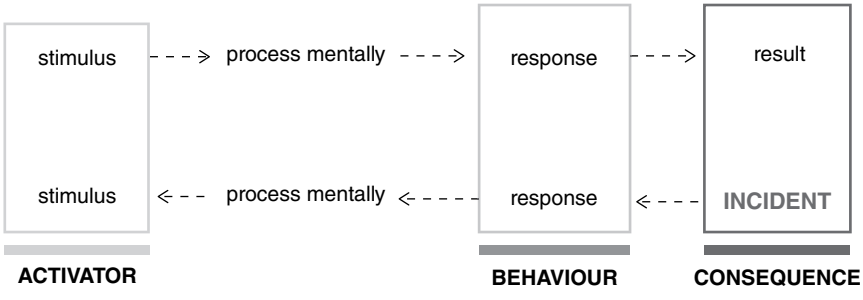


Figure 39 Stimulus-Response model. *Source:* Adapted from Fiorentini and Marmo (2018).

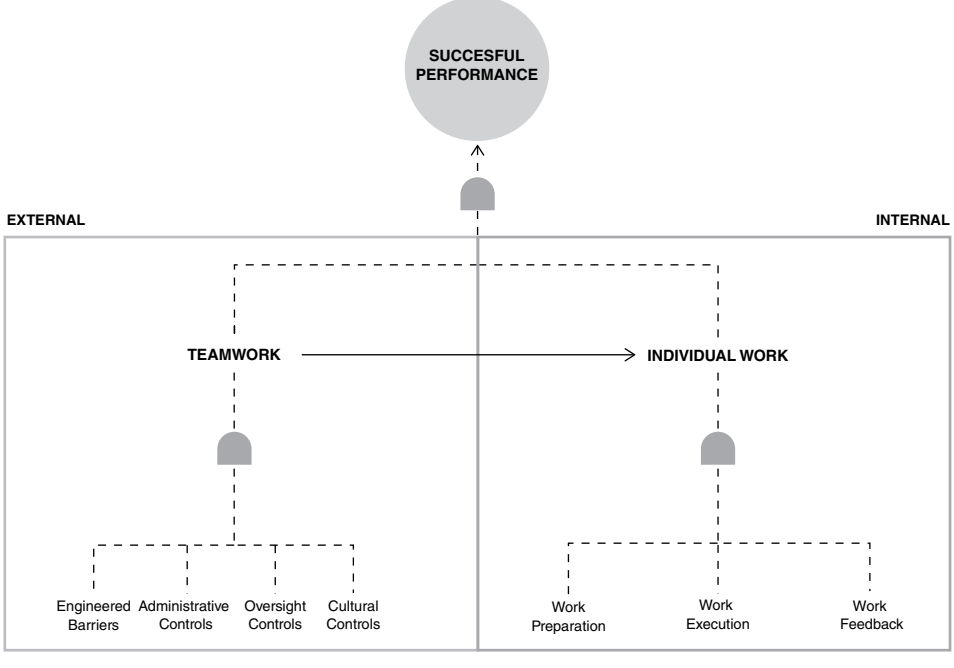


Figure 40 Two-pointed model. *Source:* Adapted from Fiorentini and Marmo (2018).

Similar to the previous model, this also, if used in reverse, becomes a tool for accident investigation as shown in Figure 41. Applying the bases of logic, AND logic doors become OR doors when they are "crossed" in reverse. Thus, starting from an incident, it is possible to have a sort of predefined logic trees (in fact very similar to fault trees) specifically addressed to the analysis of human factors.

An interesting model on human information processing is the one cited, among others in Strobhar (2013) and reported in Figure 42.

According to this model, a process that undergoes a generic disturbance $w(t)$ produces a $y(t)$ output signal. When the output signal diverges significantly from its reference value $r(t)$, then the operator detects the change $e(t)$, identifies the cause and compensates the deviation from the reference value, thus introducing a change $u(t)$ to the process himself. What matters about this model of human information processing is the "black-box" represented by the operator, where the three fundamental actions of detection, identification and compensation take place. The most attentive reader will have noticed a certain overlap with the "Detect - Decide - Act" model at the basis of the barrier-based approach, so that the two models are in fact the expression of the same perspective that can be applied because the barrier-based approach also contemplates behavioural barriers (i.e. those that rely 100% on human intervention). Any inefficiency in one of these three phases, certainly

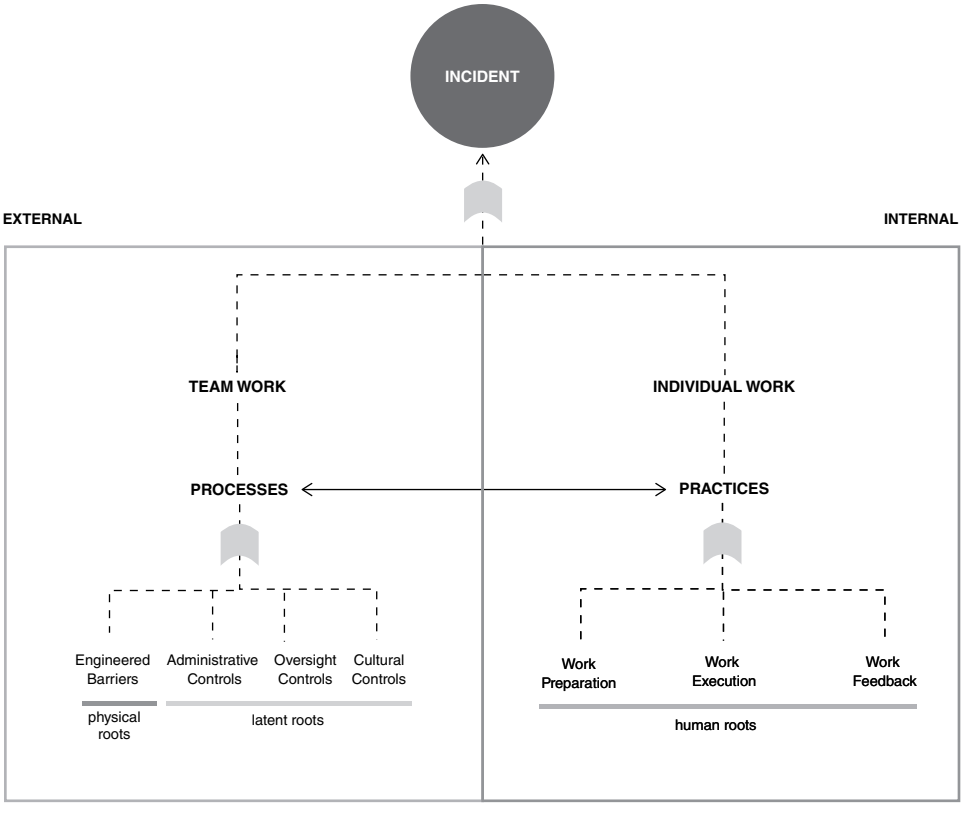


Figure 41 Inverted two-pointed model. *Source:* Adapted from Fiorentini and Marmo (2018).

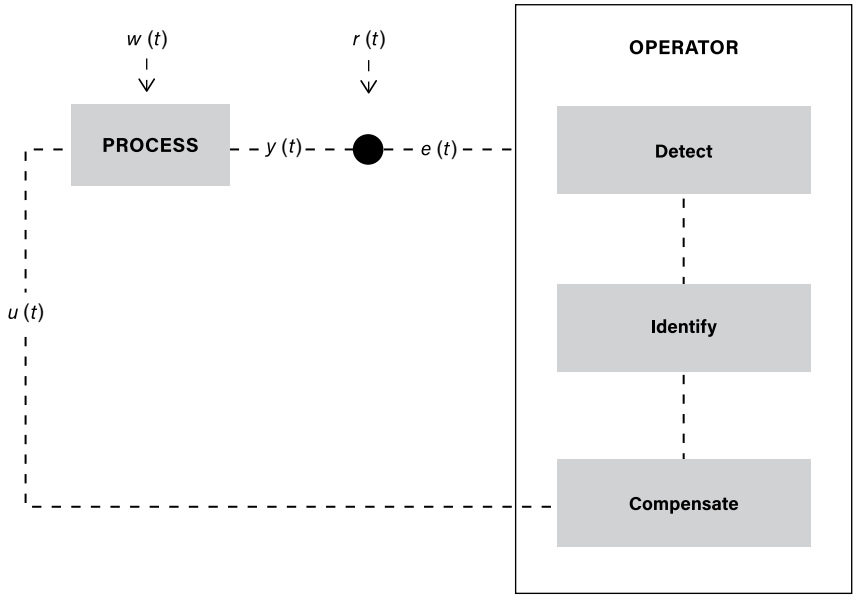


Figure 42 Human factors in process plant operation. *Source:* Adapted from Strobhar (2013).

conceivable since human intervention is far from being perfect, implies, like any barrier, including technological barriers, the assignment of a Probability of Failure on Demand value different from 0.

1.4.1 Performance-Shaping Factors

The multidimensional nature of human performance represents both an advantage and a disadvantage in the definition of human factors. How well a person performs a task cannot be attributed to a single factor, since the ultimate result of human performance is the product of several variables, often interacting with each other. One of the advantages of such a multidimensional approach to human factor analysis is the possibility of using a variety of tools to improve human performance, where required, to act on one or more specific variables. In many cases, deficient aspects in one variable can in fact be compensated for by modifying another dimension.

However, this approach brings with it at least two disadvantages. First, very often weaknesses in human performance are not directly addressed as they should be. Providing for additional training, adding alerts, or drafting longer procedures is a quick solution to solve an operator's performance problem, but only a thorough investigation can reveal the true root causes of performance degradation and thus offer cues for a more effective solution. Secondly, weaknesses in human performance rarely have simple and absolute answers because of the interaction between the various dimensions. For example, think of the interaction between training and ergonomics (i.e. the human-machine interface): the higher the level of information possessed by a user, the less information has to be replicated on a control system display.

Although there are a variety of ways to classify the variables that describe the dimension of human performance, it is common to refer to the following six dimensions (also known as performance-shaping factors):

1) *System automation and demand*. This factor takes into account, for example, control systems, alarms, and, more generally, the philosophies of automation of business processes by automated systems.
2) *Personnel and workload*. This factor includes the number of individuals involved in carrying out a given task and their relative workload, both mental and physical. Two aspects must be borne in mind:
   - Both an excessively high and excessively low workload can degrade the level of performance.
   - Increasing the number of staff reduces the individual workload, but increases the demand for team coordination.
3) *Man-machine interface*. This factor is intended to group together aspects related to the organization, content, and "shape" of the information needed by an operator to interface with a machine. This category includes aspects of ergonomics, rationalization of alarms, and design of command and control panels. The ultimate aim is to always provide the right information, in the right format, at the right time and with the right timing.
4) *Personnel selection and training*. This factor aims to examine aspects related to personnel selection procedures and methods, training programmes, skills and knowledge requirements for carrying out a task, as well as identifying training material and tools.
5) *Work organization*. Even the smallest task is part of a complex organizational process that may involve several functions within the company. It is in fact the organization that establishes expectations and tasks to be performed, therefore the way work is organized impacts on its performance. This factor includes the organization of personnel (e.g. in shifts), the creation of work teams, the identification of unitary operations and so on.
6) *Procedures and operational instructions*. This last performance factor plays a predominant role in what Rasmussen identified as the rule-based performance level (Rasmussen, 1983). In general, complex organizations today make great use of operational procedures to guide human intervention in their tasks. Therefore, since the procedures are themselves written by men (and therefore imperfect) it is essential to take this variable into account as well.

1.5 Enterprise Complexity and (Advanced) Risk Management (ERM)

Keeping in mind the principles of RM, shown in Figure 43, advanced RM can be introduced.

Enterprise risk management (ERM) is the set of organizational practices, corporate culture, and skills that an organization sculpts within its strategy and applies daily with the aim of managing risks by creating and preserving value. It is extremely important in strategic planning, because risks influence all departments and functions, aligning strategy and performance across the organization.

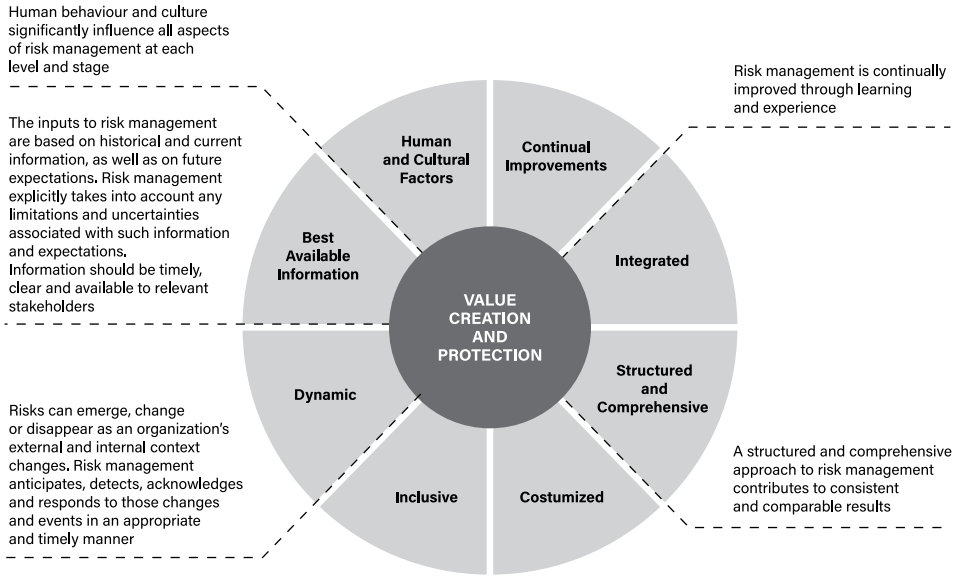


Figure 43 The principles of RM according to ISO 31000.

The main guidelines on ERM are offered by the Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2017), to which the discussion of this paragraph adheres. ERM can be defined as a process that involves all people at each level of an organization and is applied on a strategic basis at each level or unit, with an inclusive character, in order to identify potential events that, if manifested, could damage the organization. The ultimate goal is therefore risk management according to risk appetite and tolerance, providing reasonable (but not absolute) assurance to top management, and achieving the organization's objectives in one or more categories.

To do this, the structure of the ERM is based on five solid components:

1) *Governance and culture*. The former includes the organization's effort in establishing the tone, the importance, and the responsibilities of ERM. The latter refers to the ethical values and the desired behaviours related to ERM.
2) *Strategy and objective-setting*. The ERM is aligned with the strategy and objectives set in the strategic planning process. This component is intimately connected with the risk appetite of the organization (i.e. the level of risk that an organization is willing to accept), which is established and aligned with strategy, while the objectives are the practical reflection of the basis for responding to risk.
3) *Performance*. The identified and assessed risks are prioritised according to the acceptability/tolerability criteria that have been established in the context of the risk appetite. The amount of risk that the organization has assumed is then reported to stakeholders.
4) *Review and revision*. The ERM performance needs to be periodically reviewed and revised when the ERM components are substantially changed over time.
5) *Information, communication, and reporting*. ERM is also based on solid and shared information which flows across the organization. This component is therefore as essential as the others.

These five components of the ERM structure are in turn based on 20 principles, applicable to any organization regardless of size, type or business sector. Thanks to them, the ERM structure as defined by COSO can be adapted to the specific needs of an organization, based on its context and other endogenous and exogenous factors.

The following is a description of all 20 principles as provided by the COSO's executive summary (COSO, 2017).

Governance and Culture

1) Exercises Board Risk Oversight—The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
2) Establishes Operating Structures—The organization establishes operating structures in the pursuit of strategy and business objectives.
3) Defines Desired Culture—The organization defines the desired behaviors that characterize the entity's desired culture.
4) Demonstrates Commitment to Core Values—The organization demonstrates a commitment to the entity's core values.
5) Attracts, Develops, and Retains Capable Individuals—The organization is committed to building human capital in alignment with the strategy and business objectives.

Strategy and Objective-Setting

6) Analyzes Business Context—The organization considers potential effects of business context on risk profile.
7) Defines Risk Appetite—The organization defines risk appetite in the context of creating, preserving, and realizing value.
8) Evaluates Alternative Strategies—The organization evaluates alternative strategies and potential impact on risk profile.
9) Formulates Business Objectives—The organization considers risk while establishing the business objectives at various levels that align and support strategy.

Performance

10) Identifies Risk—The organization identifies risk that impacts the performance of strategy and business objectives.
11) Assesses Severity of Risk—The organization assesses the severity of risk.
12) Prioritizes Risks—The organization prioritizes risks as a basis for selecting responses to risks.
13) Implements Risk Responses—The organization identifies and selects risk responses.
14) Develops Portfolio View—The organization develops and evaluates a portfolio view of risk.

Review and Revision

15) Assesses Substantial Change—The organization identifies and assesses changes that may substantially affect strategy and business objectives.
16) Reviews Risk and Performance—The organization reviews entity performance and considers risk.

17) Pursues Improvement in Enterprise Risk Management—The organization pursues improvement of enterprise risk management.

Information, Communication, and Reporting

18) Leverages Information Systems—The organization leverages the entity's information and technology systems to support enterprise risk management.
19) Communicates Risk Information—The organization uses communication channels to support enterprise risk management.
20) Reports on Risk, Culture, and Performance—The organization reports on risk, culture, and performance at multiple levels and across the entity.

The principles of ERM, as defined by COSO, can be observed from an ISO 31000 perspective. This provides an important opportunity for organizations to better integrate risk management and strengthen the activities related to the rest of business processes. Also, this integrated approach would allow ISO 31000 principles to provide an approach for the definition of the necessary risk-based actions to ensure growth and greater economic assurance for the organization.

From the ERM perspective, successful risk ranagement requires (Louisot and Ketcham, 2014):

- A full understanding of the emerging risks;
- The definition and understanding of the risk appetite;
- Accounting for extreme events, such as unexpected large deviations from the ordinary, like a fat tail (the probability distribution that displays a large skewness or kurtosis in comparison to a normal or exponential distribution) or a black swan (an event which can have high impacts, but whose probability of occurrence is low);
- Assessing and aggregating all risks, implementing a "portfolio approach";
- Considering qualitative tools and sound judgement;
- Broadcasting the risk culture across the organization.

There are four main types of business risks to take into account in the ERM (Figure 44). They are:

1) Strategic risk;
2) Financial risk;
3) Compliance risk;
4) Operational risk.

Strategic risks affect the capability of an organization to achieve its objectives. Examples include reputational risks, risks to market presence, lack of acceptantc in the marketplace of a business plan, change in customer demands, changes in technology, or competition with other businesses. Basically, strategic risks are associated with the correct (or incorrect) application of business strategies and the ability to change them when any changes in the external or internal context happen. Facing positively the strategic risks is the key of vey successful multinational companies.

Financial risks concern the organization's ability to fulfil its financial obligations. They are mainly divided into three families: the exposure to changes in market prices, the actions (and transactions) with other organizations, and the internal organizational failures (Bansal, Kauffmann, Mark and Peters, 1991). Investment, market risk, interest rate risk, exchange rate risk, liquidity risk, and inflation risk are types of financial risk that should be considered.

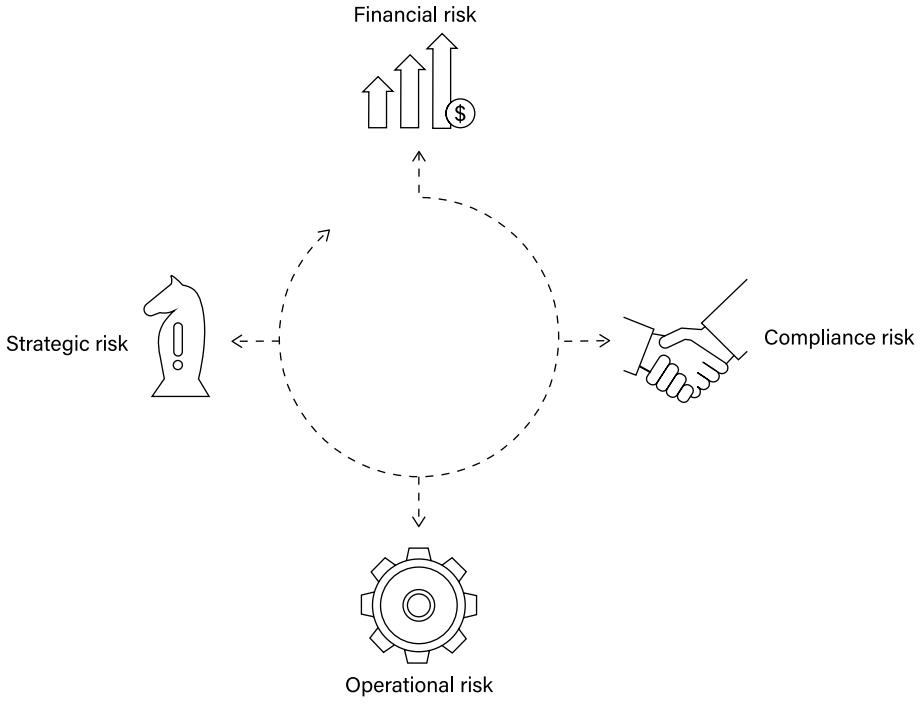


Figure 44 Main types of business risks.

Compliance risks are about the failure to act in accordance with the laws, regulations or internal policies. They are the legal penalties that an organization might be exposed to when compliance obligations are not met. This category includes (from a compliance perspective) the environmental risk, the occupational health and safety risk, the corrupt practices, and the social responsibility and quality issues.

Finally, the term operational risks refers to the failure to achieve the intended outcomes from the operations of the organization. They might come from inadequate procedures, policies or systems. Poorly faced operational risks may lead to reputational or other financial risks. Since operations are the daily basis of any organization, an effective operational risk management is essential to guarantee the prevention and mitigation of the most common type of risks, supporting the organization in achivieng its operational objectives.

A more exhaustive set of enterprise risks is shown in Figure 45.

1.6 Proactive and Reactive Culture of Organizations Dealing with Risk Management

1.6.1 Risk Management between Fulfilment and Opportunity

In order to understand the importance of the risk management culture (Figure 46), it is necessary to identify in advance its relationship with the processes to which it is (or should be) applied.

Figure 45 Most common enterprise risks.

If, in fact, the purpose of an organization is to pursue the maintenance and growth of its assets, whether material or moral, the quality level of risk management, and therefore the degree of commitment to its implementation, will be justified to the extent that it contributes value to the organization, in terms of ensuring conservation or growth.

In summary, and however cynical the statement may seem, the cost of risk management – as the use of means and resources – and therefore its level of quality, must find remuneration in the value it is able to guarantee to the organization.

It is probably easier and more immediate to associate the concept in question to an entrepreneurial organization where, through financial parameters, it can be easy to measure the cost of risk treatment and the expected and actual benefit on the managed processes.

The concept is indeed equally coherent for a moral organization; consider, for example, the reputational value and the negative effects that the conduct of a representative could generate if it is not in line with the institutional policies of the organization itself, even more so if the organization is not able to remedy it in a preventive or corrective manner.

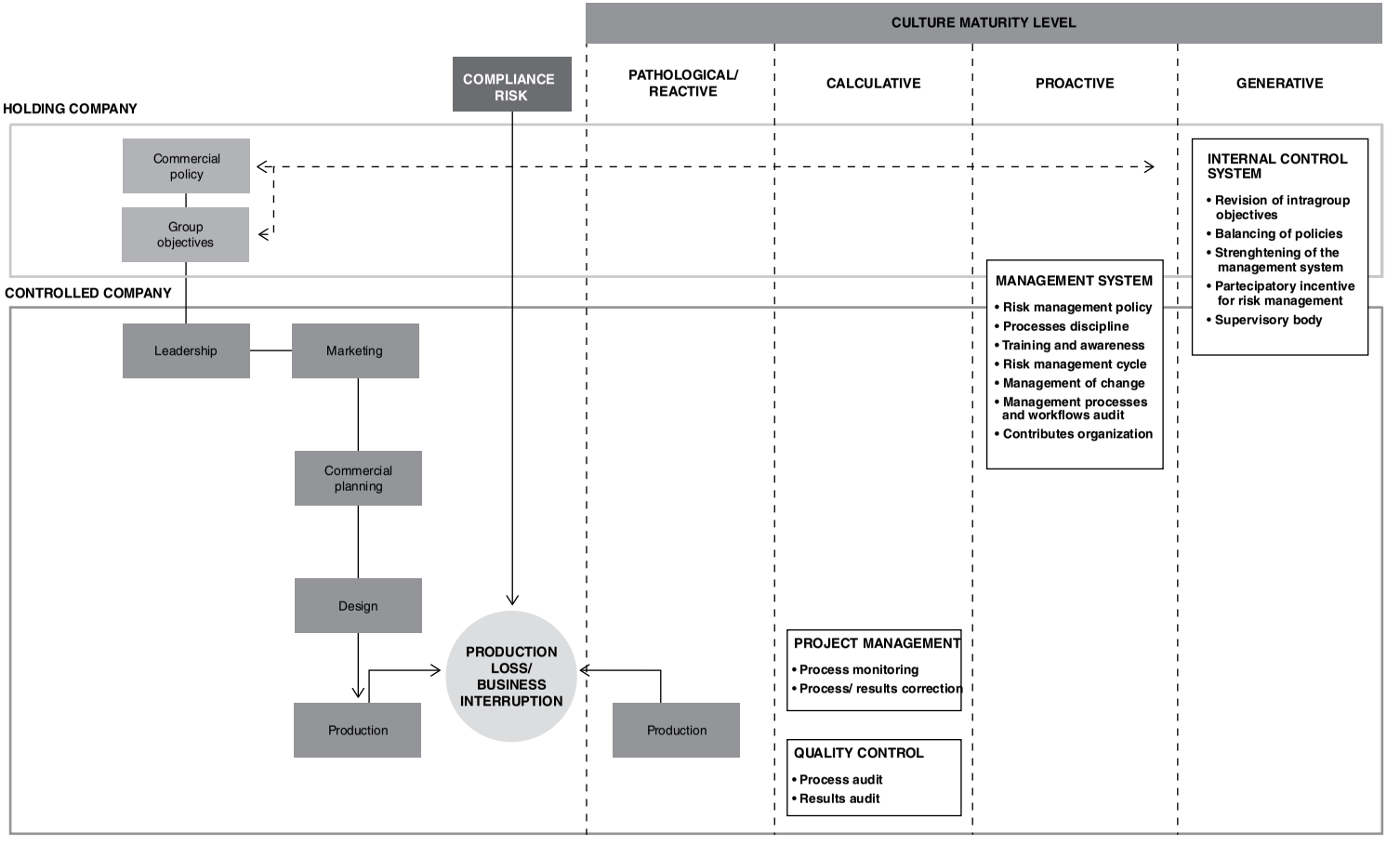


Figure 46 Culture maturity level in an organization.

From these considerations it is possible to derive, as a first and immediate consequence, that risk management can, or even better should, be framed as a normal component of all the technical and managerial management processes of the organization, rejecting any "ethical" approach to risk and ignoring that its treatment is limited to dedicated sectors of the organization but often "separate" from its ordinary operating cycle.

Talking about risk management as a separate process with respect to the functioning of the organization is in fact a risk in itself:

- On the one hand, it ends up depriving risk analysis of the technical contribution and vision in which a given objective is framed, focusing attention on the result and relegating the risk profile to an external factor to have to consider, perhaps on the basis of regulatory constraints.
- On the other hand, in the dialectic of the organization, it polarizes the role subjectivities, creating useless, if not potentially harmful, functional antinomies with respect to the achievement of the result.

Managing the processes of the organization, in an integral and inclusive way of risk profiles, both in the organizational and operational phases, allows the enrichment of the perspectives considered in the management process and, above all, the treatment of the risk to be balanced with all the profiles of the organization, triggering a virtuous mechanism of development of the quality of management.

Let's try for example to consider the process of recovery and commercial development of a building or the design and management of an industrial production plant.

From the first point of view, that inherent to the implementation of the process, both activities, although technically different, appear as extremely complex processes involving the treatment and convergence of multiple competences and organizational roles in the sub-processes respectively entrusted.

The progress of the activity requires the identification of profiles that give order to the complexity and promote choices and priorities in the comparison of alternatives.

It is also evident how the treatment of the risk profiles analyzed in relation to the alternatives considered, in the current implementation and management perspective, allow the enrichment of the process and the optimization of the choices.

Consider, for example, the management repercussions of the design choices in the fire prevention field with respect to the development of the projects or the operating costs associated with these choices; it is quite clear that during the design phase, the interest of the project team could favour the respect of delivery times or ease of implementation, leaving management with a heavy inheritance in terms of operational or financial risk.

On closer inspection, in addition to the risk of process fragmentation, there is also the risk that the number of factors considered (including risk factors) may slow down the process; however, in application of the considerations in question, the treatment of this risk at the organizational level can appropriately assess and mitigate the profile, foreseeing intermediate phases, i.e. the organizational figures, among those involved, responsible for promoting the overcoming of possible decisional deadlocks.

In any case, the process is significantly improved as any solution adopted will have been assessed, at least with an awareness of the degree of risk taken and the commitments to be made to mitigate its impact.

From the second point of view, including the treatment of risk profiles in the process management, already in the organizational phase, allows, on the one hand, anchoring the analysis to the specificity of the initiative and, on the other hand, stimulating the contribution and responsibility of all the actors involved, making the treatment of risk an added value of the organization.

In fact, the specificity of risk analysis, integrated in the management process and in the awareness of the actors involved, mitigates, at least at an organizational level, the risk of missing or inadequate assessment of operational risks or those of overestimating them, negatively constraining the planning and management of the initiative undertaken.

Therefore, in these terms, the treatment of risk profiles is integrated within the reference process, both organizational and operational, as a transversal qualitative requirement in all phases of the process itself, losing the connotation of separateness and speciality that often distinguishes it and is, at least in power, a factor of maintenance or creation of value in the organization and results. Considering safety-related risks in an organization could identify different levels of risk management that are in strict relationship with the safety culture of the organization itself (Figure 47).

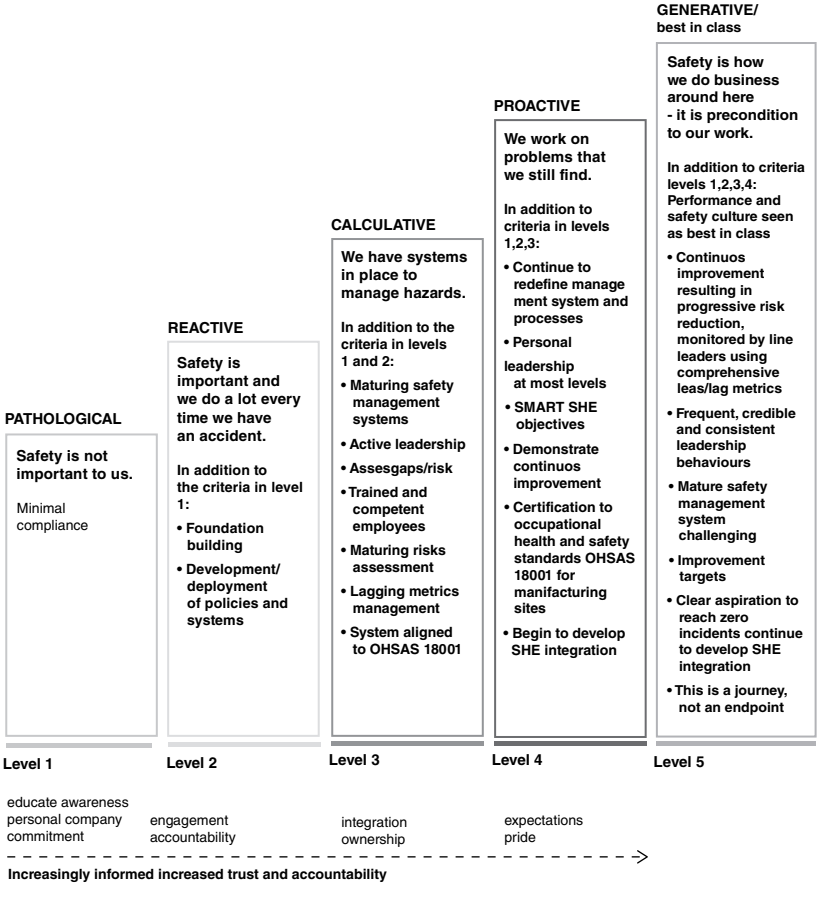


Figure 47 Safety culture levels.

1.6.2 Quality of Risk Management

With the considerations expressed, we wanted to affirm that the treatment of risk contributes to the conservation and increase of the value of the organization and in coherence with this contribution, risk management can be a qualitative component of the organizational and operational processes of the organization.

In this perspective, risk management on the one hand implements and enriches the contents of the organization's processes and, on the other, creates the conditions for a participatory approach to risk management that mitigates the risk of subjective polarization in the implementation of operational processes and, above all, creates the conditions to produce further value through the recovery of existing production.

Let us now try to make this last profile explicit and by applying the concept with respect to the path of growth of a human being, aware of all the approximation of the comparison but confident of the support that an empirical reference to a case of common knowledge can offer.

At a few years old a child starts walking; he or she stumbles or collides with objects, either stationary or moving, on his or her path because they are not properly considered.

Progressively, with a series of falls and some crying, the child increases his skills, and reacts by learning to recognize and evaluate objects on his path to avoid them.

Therefore, the child achieves a degree of awareness in which he or she observes the rules dictated on the basis of experience and walks with reasonable confidence in the home environment.

Furthermore, the child learns to apply the rules of experience autonomously and to interpret heterogeneous signals for walking in environments other than domestic and habitual ones.

In the end, the child pursues his or her will to walk by applying independently and automatically the rules of experience acquired and increases his or her skills by running and playing.

The example in question, whose summary and approximate character is reiterated, is however certainly useful in focusing on some concepts mentioned in the previous pages.

One learns not to fall, to walk indoors, then outdoors and then again to run and play, processing together the objective pursued and the associated risks.

In other words, an entrepreneurial organization pursues economic objectives set out in the articles of association and does not a priori manage risk; however, it is clear that the treatment of the risks associated with the objective is a component of the management process aimed at achieving the result.

Treating the risk is impossible only in association with the objective identified and the process necessary to pursue it. We can say that risk does not exist without the objective of which it remains as a sort of negative predicate.

In this perspective, the treatment of risk brings value to the organization.

In the child's developmental process, as simplistically described, objective and risk are treated in direct association, initially unconscious and mutually interfering, with the result of enabling the child to achieve the objective and setting the conditions for further development of his or her abilities.

In this path, objectives and risks continue to be treated jointly and to feed each other in a process of capacity and awareness growth that continuously recovers the bases of experience to rework them with respect to the new objectives and to identify new risk profiles to be evaluated with respect to the new objectives.

In this perspective, at a methodological level and even more so in an organization, the treatment of risk integrated in the management process brings the added value of fluidity and process efficiency through preventive and corrective remedies already integrated along the way.

Finally, we cannot but observe how, in the organic unity of our child, the rules of experience are acquired and made available to all the sensory and cognitive abilities of the person, evidently affected by the same developmental path.

We certainly do not dwell here on the interactions of this unity, but we cannot but note how the same perspective applied within an organization, or even more so within complex and mutually interfering organizations, can further contribute to the growth of the organization through the recovery and diffusion of the rules of experience, the application of the same rules on different management processes of the same organization, and the stimulus to the identification of new signals or new scenarios.

In other words, the treatment of risk, as a speculative predicate of the objectives pursued, as a process culture can offer further added value to the organization.

We therefore try to apply risk treatment in the developmental stages related to the child to an organization, classifying a series of "standard" conditions, as shown in Figure 48. In the following paragraphs, fire safety level has been used as an example of different culture levels of an organization to clarify the importance of the attitude of the organization towards risk management. This could be extended to any kind of risk that threatens the organization.

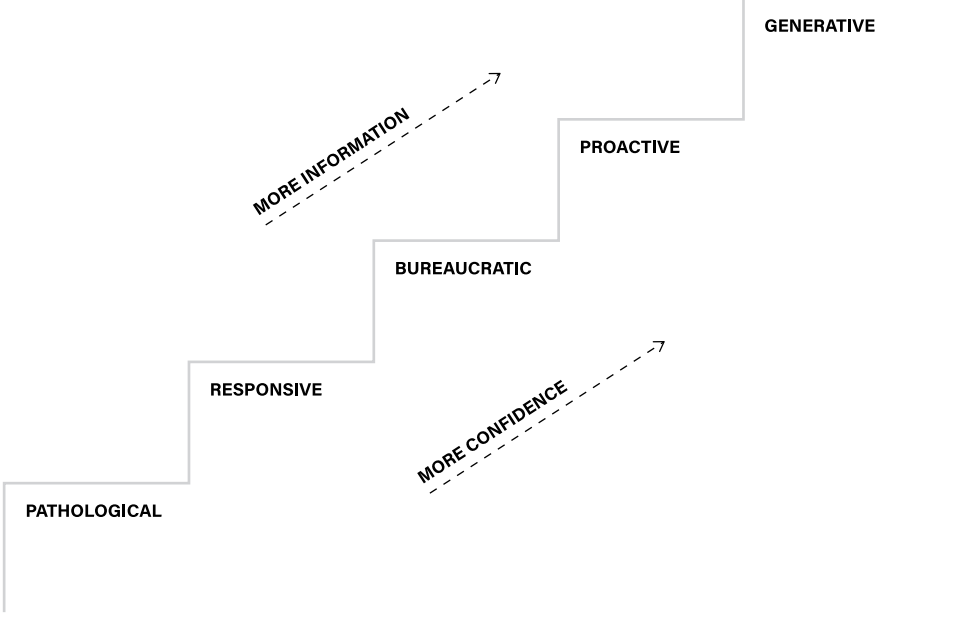


Figure 48 Quality of risk management approach.

1.6.3 The Pathological Condition

The "pathological" condition (Figure 49) corresponds to the absence of preventive risk treatment, a condition in which the organization promotes its objectives through processes aimed exclusively at obtaining results.

The organization identifies the objective and develops in a serial manner the activities deemed necessary to obtain it without consideration of the interfering factors – if not limited to those that can offer opportunities for direct maximization of the result – and therefore without the identification of preventive or subsequent corrective factors.

The management process is necessarily poor because the lack of risk treatment prevents the implementation of the analysis of the operational process, jeopardizes the possibility of developing synergies between company processes, and is characterized by the lack of information disseminated throughout the organization.

Organization objectives should be clearly identified through a specific process that also identifies the expected results; after all, the pathological condition pervades the same organizational structure, preventing a priori the preliminary analysis necessary to define the process and the expected results.

In other words, the organization wants to "walk" and starts to do so without considering the ability to sustain the necessary commitment over time, without identifying the obstacles on the path or alternative trajectories or verifying the opportunity to achieve the same objective in different and alternative ways.

The organization does not treat the risk until it manifests itself in a dangerous condition that results in damage that jeopardizes the achievement of the result.

The organization reacts within the limits of what is necessary with respect to the incidence of the damage with respect to the organization and the restoration of the operation

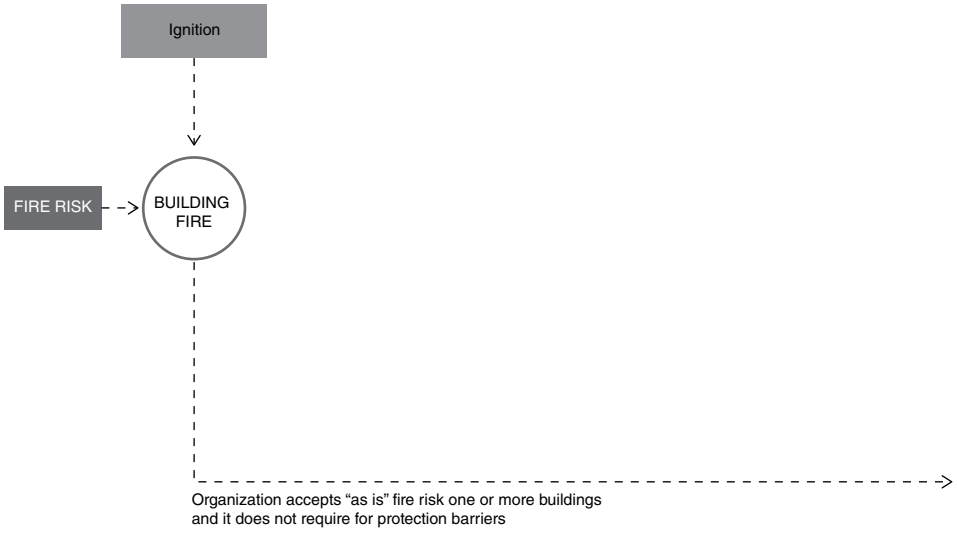


Figure 49 The pathological condition.

of the process without, however, re-evaluating its suitability and persecutability and, above all, without "capitalizing" the event by transforming it into a rule of experience to be evaluated with respect to the organization and the complexity of its processes.

One might conceptually wonder whether this is acceptance of the risk or whether the organization ignores it a priori.

The pathological condition is typical of organizations operating on processes and scenarios characterized by limited technical production constraints, market scenarios with a low competitive level, a low level of outsourcing of operational processes, and regulatory contexts that tend to be prescriptive, which would make the value contribution of risk management appear negligible.

On closer inspection, in reality, the risks of business continuity or the risk of inadequate calibration of production objectives, for example, are quite significant even in expected monopoly markets that could generate significant revenue losses or penalties with respect to the failure to meet demand.

In short, in order to answer the question about the organization's awareness, we can consider that the pathological condition – which, as indicated earlier, pervades the organizational structure and processes – is at the same time the result of a risk acceptance that is not fully aware by an organization that, even knowing it, does not accept the stimuli and does not use them to evolve, evidently endorsed by a technical, regulatory, and market context that is not particularly demanding.

It is certainly possible to affirm in this sense the correlation between the degree of quality of risk management in the organization and the reference context.

1.6.4 The Reactive Condition

If an obstacle is hit when trying to walk, the reaction will be all the more important the more significant the damage and pain suffered.

This in brief can be a description of the "reactive" condition in risk management (Figure 50).

This is a condition immediately superior – if possible identifying a line of qualitative development of the risk management culture – to the pathological condition.

The organization not only suffers damage for which it may even be sanctioned, as in the pathological condition, but in the face of the importance of the damage suffered it reacts immediately by making significant efforts to eliminate the damage suffered and align the process with the management of the risk that has occurred, integrating the process itself with corrective measures that had not been previously assessed.

This is a strong reaction, the result of the awareness acquired by the organization as a result of the damage suffered but limited to the event that occurred.

The reaction does not feed the evolution of risk management either with respect to organizational or operational processes.

As with the pathological condition, it can be assumed that, in the reactive condition, the organization has accepted the risk although with the greater awareness reflected in the intensity of the reaction.

After all, if in the organic unity of the person, evolution is dictated by the natural ability to elaborate stimuli, the satisfaction of needs, and the action of external educational and training factors, the ability of the organization to understand, acquire awareness, react to

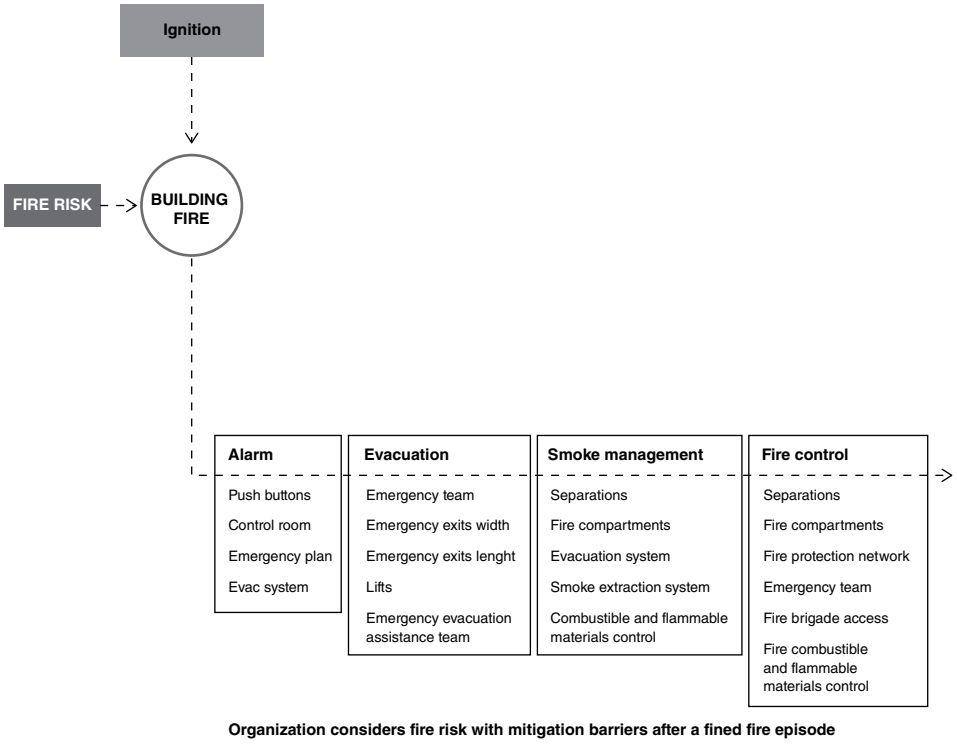


Figure 50 The reactive condition.

stimuli, and gradually evolve to "superior" conditions is the result of an artificial construction strictly dependent on organizational policies, the subjectivities responsible for management roles, and the technical, regulatory and scenario constraints in which the organization operates.

In this perspective it is possible to affirm that the reactive condition can be endorsed by prescriptive regulatory contexts in which the cases of possible non-compliance are typically outlined and identifiable and to which the strong but precise reactive approach of the organization in case of accident is adapted.

This context probably does not favour the development of risk management as a generative process of added value for the organization.

1.6.5 The Bureaucratic Condition

In the "bureaucratic" condition of risk management (Figure 51), we can clearly identify a first concrete step in the line of qualitative development of risk management in the organization.

In the bureaucratic condition the risks are consciously treated by the organization which, according to their identification, dictates the risks as preventive corrective factors.

Not only that, the assumption of the rules by the organization implies that they are disseminated to all members of the organization who must comply with them in order to prevent non-conformities and accidents.

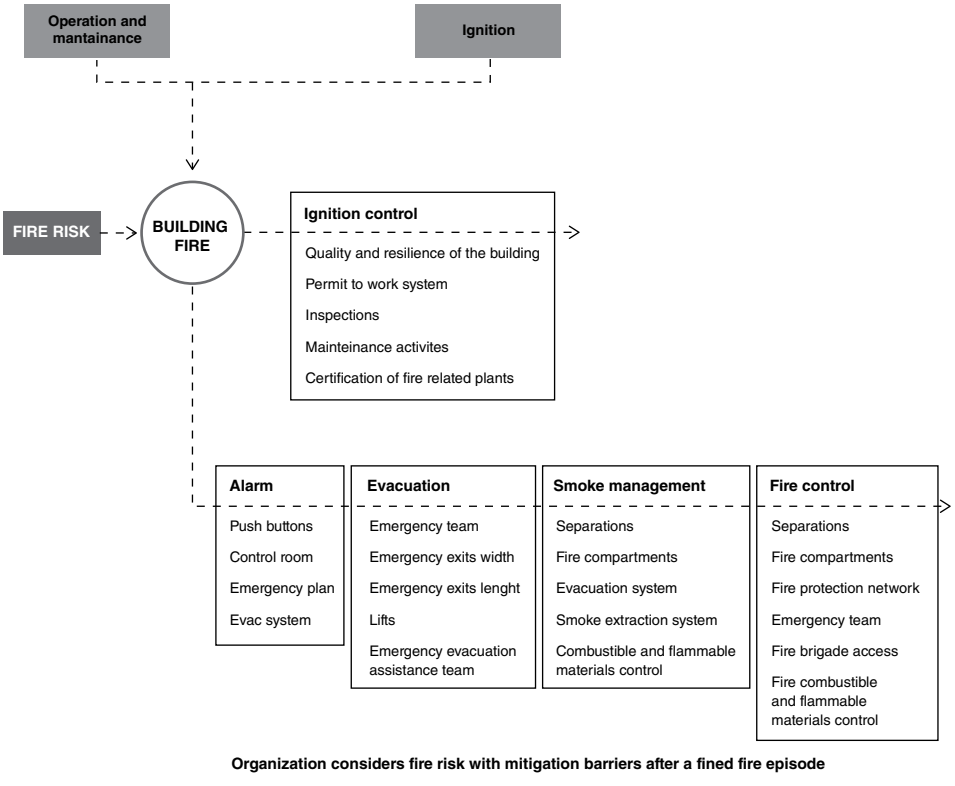


Figure 51 The bureaucratic condition.

The qualifying step of the bureaucratic condition lies in the affirmation of a risk management policy by the organization, which in turn informs and shapes the operational processes.

It is only through the affirmation of a policy that risk management takes on a systemic character in organizational and operational processes, attesting to the awareness of the organization and removing the treatment of risk from the individuals who make it up.

The bureaucratic condition definitely overcomes the grey area of pathological and reactive conditions in which risk acceptance is based on the limited awareness of the organization.

Of course, it is not that the individual members of organizations defined as pathological and reactive cannot be able to identify and assess the risks of the activities from a technical and managerial point of view; simply, that type of organization does not require it.

In the bureaucratic condition the organization manages the risk, identifying the profiles and dictating the rules that everyone must implement to avoid the dangers.

In other words, an organization in bureaucratic condition is like a child who has acquired the necessary rules to walk inside the house; it is an organization that moves with relative safety within a given perimeter and as long as all its actors respect the rules.

On closer inspection, however, it is an organization whose risk management is not flexible and does not adapt to changes in the scenario, does not produce added value, and at most guarantees the preservation of existing value as long as the context does not change.

Furthermore, it is an organization that does not seize the opportunities associated with the commitment required of its actors to comply with the rules and misses the opportunity to take and treat critically external stimuli to enrich processes or simply exploit the synergies between homogeneous processes in dealing with the corresponding risks.

Finally, precisely because of this rigidity, such an organization would not be safe in those regulatory contexts that base responsibility on risk management and that introduce the adequacy of the evaluation with respect to the accentuated complexity of the current technical and management processes, ending with the admission of an a posteriori judgement on the goodness of the management process and therefore on the conduct of the actors involved.

1.6.6 The Proactive Condition

In the proactive condition (Figure 52) there is widespread attention of the actors in the organization to the danger signals.

The organization has taken an important step forward compared to the conditions described previously. In the bureaucratic condition in fact:

- The policy has enabled awareness of the organization of risk and its treatment to be taken into account.
- Awareness generated the analysis and assessment of the risk, which in turn led to the definition of the rules.
- The rules are deliberately spread throughout the organization and everyone must follow them to avoid dangers.

In the proactive condition, on the other hand, risk awareness extends beyond the boundaries of the organizational process and informs operational processes: the actors not only follow the rules to avoid dangers and accidents, but are also attentive in advance to danger signals.

They identify the signals and react by bringing them back into the management process for their treatment and for implementing the risk management and knowledge assets.

If the precondition of the proactive state lies in the existence of a risk policy on the part of the organization (as already in the bureaucratic condition), the maturation towards the proactive condition is dictated by the organization's need to grow.

As the child, after learning to walk in the house, ventures outside into an unfamiliar environment, the proactive organization needs to identify danger signals to learn to move in new scenarios, markets, constraints and contexts, developing the process and handling of the associated risk.

One might wonder whether the detection of the danger signal is the implementation of a rule or the result of the organization's stimuli.

Probably, the delimitation between the sphere of having to do it and wanting to do it is not identifiable in a clear demarcation line.

More likely, observing an organization in concrete terms, one would end up observing a range of behaviours in which they both alternate in profiles but whose orientation, over time, towards one or the other of the spheres in question could certainly be an indication of the organization's maturity.

Of course, to speak of "will" is to be understood in any case within the framework of a system of rules dictated by the organization; it would be in other words a will progressively

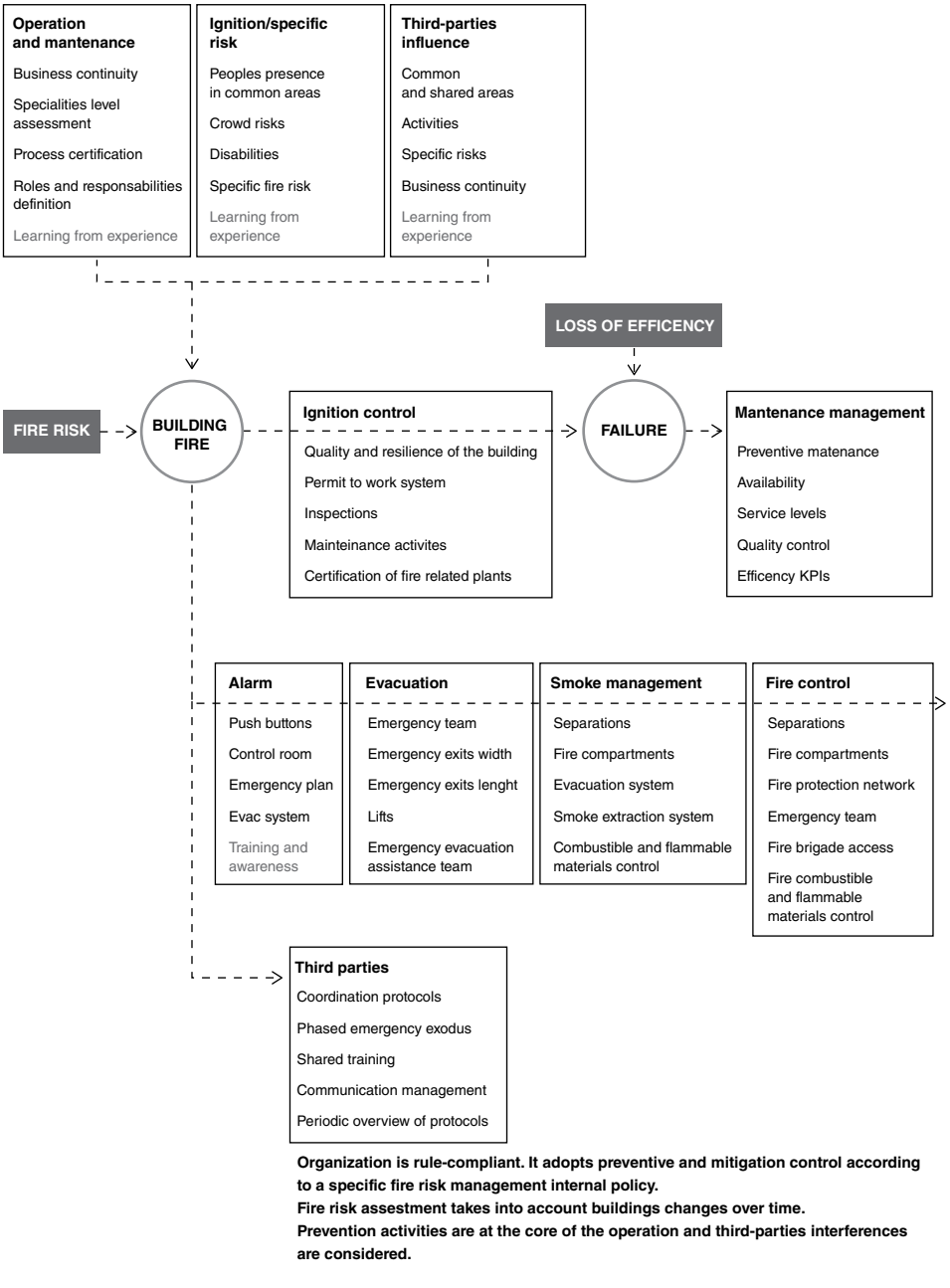


Figure 52 The proactive condition.

induced or easily obtainable by the organization as a result of the development and implementation of a policy oriented towards sharing and widespread participation in the organization.

In any case, it is clear that, as shown at the beginning, risk management in the proactive condition is able to generate value for the organization.

1.6.7 The Generative Condition

The generative condition (Figure 53) represents in some way the complete maturation of the organization, the one in which risk management is an integral part of company processes, and a factor competing with the production of value in the perspective indicated at the beginning of this discussion.

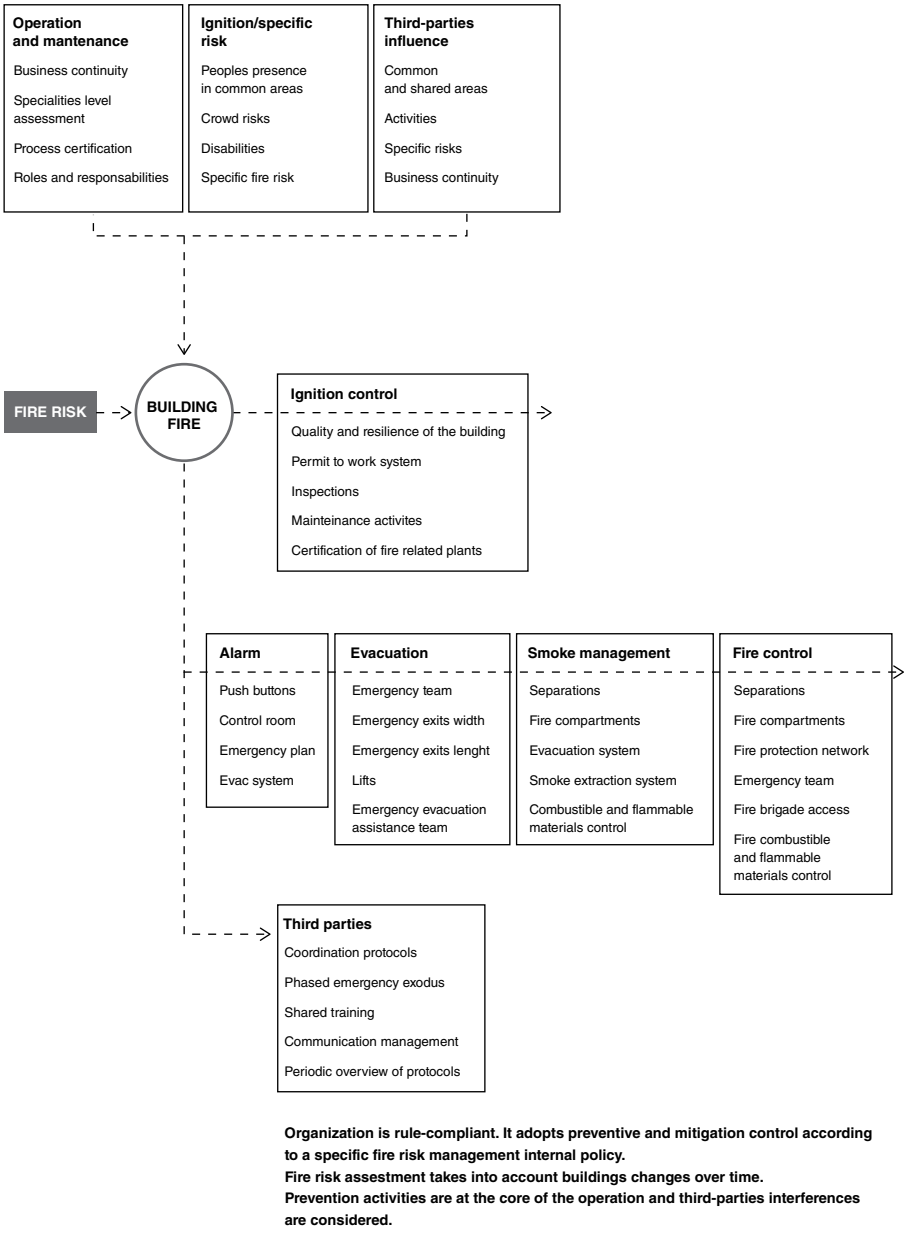


Figure 53 The generative condition.

For the condition in question – taking up again the comparison with regard to the duty of care and voluntary behaviour – the actors of the organization, whether they are involved in organizational or operational processes, naturally consider risk management to be an integral part of their activities, working, on the basis of the sensitivity induced by the organization and the training factors provided, to identify risk profiles, to implement containment actions and to contribute to updating the analysis and evaluation and, therefore, the processes.

The organization naturally develops a path of continuous regeneration based on the widespread contribution of the actors, which ends with self-feeding.

The generative condition allows the organization to adapt to changing scenarios, to deal with regulatory development with greater flexibility, and to overcome the technical constraints of operational processes.

But above all, the generative condition elevates the organization by depersonalizing it from the actors that make it up and characterizing it in terms of subjective synthesis superior to the policy pursued.

In other words, through policy and generative maturation, the organization protects itself from the risk of application deviations that can ultimately characterize the individual conduct of its actors.

In conclusion, the descriptive articulation of the degree of culture that characterizes risk management in organizations through the proposed classification is obviously a mere methodological expedient aimed at affirming the diversity and orientations that can be revealed in practice.

However, it is immediately evident that these are not imminent conditions but rather orientations of the organization in a more or less fluid condition from one to the other, depending on the degree of consolidation of the policy in its adequacy of application within the organization.

Nevertheless, the conditions described can be read as a term of reference or comparison that can offer support to the analysis of concrete situations from which to move to orient the development of a given organization towards the opportunities offered by the correct application of risk management in the perspective of value creation.

1.7 A Systems Approach to Risk Management

For many years every aspect of the organizations were treated with a deterministic approach with the precise aim of governing them with rules and detailed requirements. Organizations were seen as systems of single components. In this framework performances of organizations were directly linked with the continuity and improvement of single components of the entire system: each one with a different importance given its criticality and the effects on the outcomes. This initial approach survived up to the 1990s. Since then organizations have been recognized as entities governed by a number of different processes (primary, auxiliary and supporting processes). This new approach allowed the identification of the main flows of materials, information and data, energy, and so on across the organization, intended as a system with specific objectives and processes organized in areas and sectors (commercial process, production, customer support, etc.), each one having its own key

performance indicators (KPIs) to be reviewed periodically. Organizations became systems composed of processes and elements. Processes could be governed by procedures rather than with specific prescribed requirements to be followed to achieve performance. Organizations were requested to learn from negative occurrences and deviations from intention and to measure the increase or decrease related to the objects in one or multiple domains. Increases have been identified with the improvement to be maintained over time in a circular scheme known as Plan-Do-Check-Act (PDCA) (see Figure 54), where the failures from planned intentions should be avoided with preventive actions and non-conformities management, both raised by a specific audit program whose results should be taken to the attention of top management and any eventual stakeholders.

This systemic approach to processes (internal and external) governed organizations up to 2015, when it was completely replaced by a risk-based approach. Processes are the atomic unit of an organization, but deviations (with the limitation in the extent of achieving the desired performance) are connected to a number of internal and external conditions; it is quite difficult to associate each single deviation to the failure of a single element of the process and the deviation from the organization objectives is likely to be linked to a number of perturbed situations rather than the failure of a single process (even if a primary and vital one). Single deviations could lead to disruptions in other correlated processes and small ones, cumulatively, could lead to severe problems with a significant loss of performance. The initial theory of component failures can describe the single element, and the subsequent process theory can describe deviations inside the primarly affected process and those few directly linked (in input and in output) to that. Real incidents, deviations, and anomalies are useful in describing the local problem. In any case real episodes with impact cannot be easily understood and organizations are not able to improve taking advantage of the learning from experience transversal knowledge process. Lack in efficiency has been discovered to reside in the impossibility to deal with complexity that characterize every domain of application. Complexity poses risks with a potential impact on components and processes, and both of them, and risks, take advantage of shared vulnerabilities and the human factor (including the error probability of human-centered processes, tasks,

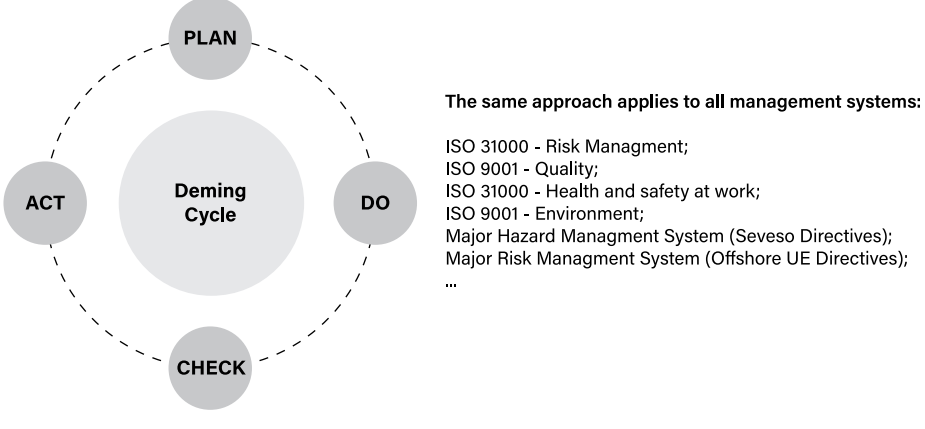


Figure 54 The Deming Cycle PDCA.

operations). With such complexity it is not possible (not only because it is too time-consuming) to identify all the possible outcomes (especially impact) of all the possible deviations. Impacts also could be directed at the same time towards different vulnerable receptors with a different degree of severity. This awareness raised the need to deal with complexity (in an always-evolving reality) using a risk management approach. The ISO 31000 standard, especially in its more recent edition, became the kernel of organization management across different domains. Organization management systems turned from a process-centered perspective to a risk-centered perspective and the latest objective of each single organization is risk management as the core activity to avoid failures, disruptions, and so forth. Successful organizations are those that can prove to be risk-resilient to top management and stakeholders. The risk management process embraces all the processes of the organization and is conceived with the right focus and zoom level to manage systematic issues and single-element performance, considering their relative criticality in the overall picture. Improvement comes from risk-based thinking and actions are identified, selected and put in place according to their estimated risk reduction factor. Since risk is an effect of uncertainty on objectives (deviation from expected), two pillars should govern modern organizations that are willing to manage risks to take better decisions: risk assessment (composed of risk identification, analysis and evaluation phases) for the risks to be treated and periodic monitoring and review, including reporting and communication activities. With this risk management process, it is possible to design a strategy for complexity and it is also possible to learn from real experience, as well as modify the risk management approach considering new, emerging, and underestimated risks. Complexity management means risk reduction and control for those risks arising from the known internal and external contexts, against specific risk criteria defined by rules (in certain domains) or by the company (according to the willingness to preserve assets and create more value). A systematic approach to organizations defined as systems has to be based on risk analysis. The purpose of the analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. It involves a detailed description of a number of factors: likelihood of events and consequences, the nature and magnitude of impacts, complexity and connectivity, time-related factors (including volatility), the effectiveness of existing controls, sensitivity and confidence level. Subsequent risk evaluation should support decisions: Are available controls sufficient? Should new controls be put in place? Should existing controls be maintained? Risk management creates and protects value. It contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, legal and regulatory compliance, environmental protection, product quality, efficiency in operations and business continuity, governance and reputation, and so on. Therefore, the process to manage risk should be an integral part of the activities that generate risks. It should be systematic and structured and also based on the best available information. If controls, as the reader will observe in this book, are the barriers to avoid or lower the probability of an undesirable outcome, then the risk management process should be dedicated to barrier management in a way that both physical and human barriers act on risks and technological and human threats are managed over time to avoid any undesired impact on vulnerable assets. Risk management avoids the failure to recognize complexity and allows the organization to improve even during real incidents, since for each of them, root cause analysis of the factors that affected

one or more risk control failure are identified. Risk management (aka barrier management) is dynamic, iterative and responsive to change. It continually senses and responds to change. As internal (and external) events occur, internal (and external) context change, monitoring and reviewing risk take place, new risks emerge, some change and others disappear. Controls are reviewed to ensure their ongoing effectiveness in response to change. Monitoring and review activities are fundamental to keeping the risk management process in place and effective.

Specific and distinctive activities should be put in place to assure that assumptions, results and related decisions remain valid over time and, if not, that a management of change process is in place and considers risk management activities. These activities are known as "monitoring" and "review" of the risk management process.

- Monitoring involves the routine surveillance of actual performance and its comparison with expected or required performance. It involves continual checking or investigating, supervising, critically observing, or determining the status in order to identify change from the performance level required or expected, as well as changes in context.
- Review involves periodic or impromptu checking of the current situation for changes in the environment, industry practices, or organizational practices. It is an activity undertaken to determine the suitability, adequacy, and effectiveness of the framework and process to achieve established objectives. Reviews should consider the outputs from monitoring activities.
- An audit is a process of evidence-based, systematic review against pre-determined criteria. While every audit is a review, not every review is an audit.

As defined in Annex E of the ISO/TR 31004 guide, risk management is (and should be) part of an organization management system. In modern organizations the integration of a risk management process into the organization's system of management should ensure that risk assessment is used as the basis for risk-informed decision-making at all levels of the organization. Many internationally recognised standards deal with management systems in general or, as readers will see, with regard to a specific content. Formalised management systems consist of requirements that provide a consistent framework in which the organization can establish sound practices and procedures to direct and control its activities. Risk management adoption in modern management systems increases the focus of top management and stakeholders on the organization's objectives and enable all risks in an integrated management system under the principles of the ISO 31000 standard that are fully compliant with the PDCA approach of the majority of recognized management systems. Nowadays it is possible to affirm that risk assessment is a formal key element of modern management systems, as a means to deal with specific complexities the organization should face to achieve the intended performance.

In the following paragraphs a glimpse of the most adopted management systems is given.

As the descriptions of those management systems show, risk assessment is an activity to be fully integrated in the management process and it comprises the core elements of the risk management process; it contains the following elements:

- An established context;
- Risk assessment (identification, analysis and evaluation);

- Risk criteria;
- Risk treatment;
- Monitoring and review;
- Communication and consultation.

These elements are pillars of each management system and, as readers will observe in the next chapters, the Bow-Tie is a simple diagrammatic way of describing and analysing the pathways of a risk from threats to impacts and reviewing controls. It allows a quantitative consistent output. According to this root cause analysis (especially in the format of barrier failure analysis) is a simple way to understand contributory causes and how the system (and associated processes) can be improved to avoid such future losses. This analysis considers existing controls/barriers (in place at the time of the deviation) and how they can be improved. It also allows a quantitative evaluation in terms of probabilities of failure on demand (PFDs) and risk-reducing factors (RRFs). Both the tools could be coupled with a LOPA, also called barrier analysis, that allows controls and their effectiveness to be evaluated. Those three techniques, referenced in IEC 31010, combined can help in satisfying the requirements of the modern management standards that specifically require, in the domain of application, a significative risk-based thinking.

If decisions arise from the consideration of results of a risk assessment, risk is a key element that can be considered common to all the management systems in place and included in each specific domain.

The "risk" element becomes part of all the core business processes: this raises and underlines the need to create interaction between all the management system approaches, among them quality, environment, compliance, energy, management, and so on, supported by their domain-specific management systems. The individual management system, considering risk management as a common and shared fundamental element, should form a single and integrated management system where a single policy could face several aspects and objectives are those of the entire organization. Integration can take advantage of a common structure of the latest edition of the domain-specific standard on management systems: this approach could lead to lean implementations and to important savings with more effective and documented results. Furthermore it is possible to notice that some threats have an impact on multiple different domains (e.g. a safety incident determining a loss in terms of people, environment, assets, business continuity, a cyber threat with an impact on different organization processes such as customer relationship management, supply chain, etc.): having a single shared organization risk register would lead to a better understanding of the risk profile of the organization, towards the adoption of an enterprise risk management framework. A single risk register could be easily maintained and updated and it could become a single point of access to all the stakeholders, eventually through specific KPIs and dashboards. In any case a single risk register doesn't request that a single methodology be used for the assessment of the various specific threats, while it could be used the receptor of normalized results, whereas, on the contrary, barrier-based risk management methods and tools (such as Bow-Tie and barrier failure analysis) could be seen as an opportunity to deal with a number of risks with a standard and ISO 31000 compliant approach, both during the design phase and over time.

Compliance with legal requirements (including an organization's internal standard) is mandatory for all the management systems: controls (barriers) must be established to

ensure that it is a vital part of the management system regardless the themes to be managed. Furthermore, quality aspects should be guaranteed even in the risk management framework. Given these two examples it is obvious that risk-based thinking is the key element of various management systems, but to be successful it should be as practical as possible: if old prescriptive codes were too specific and not able to face the change, they were simple and straightforward. The success of risk-based management systems is strictly related to the underlying risk management process and its maintenance over time: non-identified risks or non-evaluated risks could pose severe impacts to a number of organization processes. Risk-based thinking and risk-based decisions require a strong commitment from leadership and the full involvement of human resources, with all the associated issues, as the need for competence and training, their periodic assessment, and so forth.

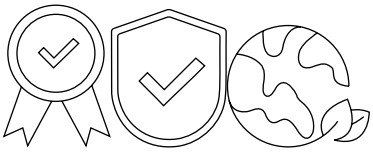
It is important to notice that risk-based standards ease this integration of risk management practices adopting a common structure, composed by a number of common elements that work in the PDCA general framework. A management system is a set of policies, processes and procedures used by an organization to ensure that it can fulfill the tasks required to achieve its objectives. These objectives cover many aspects of the organization's operations (including financial success, safe operation, product quality, client relationships, legislative and regulatory conformance and worker management). Many parts of the management system are common to a range of objectives, but others may be more specific. A complete management system covers every aspect of management and focuses on supporting the performance management to achieve the objectives. The management system should be subject to continuous improvement as the organization learns (return of experience).

Elements may include:

- Leadership involvement and responsibility.
- Identification and compliance with legislation and industry standards.
- Employee selection, placement and competency assurance.
- Workforce involvement.
- Communication with stakeholders (others peripherally impacted by operations).
- Identification and assessment of potential failures and other hazards.
- Documentation, records and knowledge management.
- Documented procedures.
- Project monitoring, status and handover.
- Management of interfaces.
- Standards and practices.
- Management of change (included project management).
- Operational readiness and start-up.
- Emergency preparedness.
- Inspection and maintenance of facilities.
- Management of critical systems.
- Work control, permit to work, and task risk management.
- Contractor/Vendor selection and management.
- Incident reporting and investigation.
- Audit, assurance and management system review and intervention.

Management systems should be documented with a specific set of evidences. The number and content of management system documents is not predefined, but rather is defined on the basis of the needs identified (in this case using a risk-based approach with the assessment of the impact following the lack of a document). The hierarchy of the selected documents is quite common and from top to bottom it is built around policies, the system manual, procedures, standard operating procedures (SOPs) and work instructions, records and forms (templates and filled forms). This generally adopted hierarchy does facilitate the integration of various management systems.

1.7.1 ISO 9001 (Quality) / ISO 45001 (Occupational health and safety) / ISO 14001 (Environment)



Among the most recognized and adopted management systems, specific attention should be given to ISO 9001, ISO 45001, and ISO 14001 management systems, which can be certified by third parties. They face aspects that are quite common to the majority of the organizations, respectively, quality, occupational health and safety, and environment. These standards will be discussed, for the goals of this book, together since, in their latest edition, they share common structure, definitions, and language.

The main objective of any modern organization is the creation of value within the company and its protection over time. The path towards this goal requires facing internal and external factors that influence, negatively or positively, the organization's ability to achieve it on a daily basis and making decisions on the consequent strategic actions to be implemented.

The decision-making tool that the organization uses to achieve this objective is the management system; according to the definition of ISO 9001 a management system is a "set of related or interacting elements ... aimed at establishing policies, objectives and processes to achieve these objectives." According to the given definition, the management system supports and guides the organization, usually its leadership, in the identification of these internal and external factors that influence its daily action, in the identification of significance, in terms of influence on the ability of each one to achieve the objective and, ultimately, as a decisional tool, in the identification of actions to be implemented to maximize positive influences and minimize negative ones.

In general, the ability, and the possibility, to achieve any objective is affected by a margin of uncertainty (and risk has been defined as the effect of uncertainty on objectives).

According to the definition of the latest version of these common ISO (9001, 14001, 45001, 50001), standards aligned with the HLS – High Level Standard Systems, the effect of this uncertainty, intended as a positive or negative deviation from what is expected (note 1), is the "risk."

Incidentally, note 4 to the definition provides a less qualitative indication of how this risk is made: "... Risk is often expressed in terms of a combination of the consequences of an event ... and the associated likelihood ... of occurrence."

The strategic action of the organization, or of its leadership and top management, must necessarily include knowledge and awareness of the uncertainty and, therefore, of the associated risk. To this end, within the harmonized approach introduced with HLS, the concept of risk-based thinking is implemented through clause 6.1, "Actions to address risks and opportunities," which we find in all standards, regardless of the specific considered domain (quality, safety, environment, or energy).

Some considerations on how to comply with the requirement:

- In all standards, the requirement is made explicit in general terms "... the organization must determine the risks and opportunities that need to be addressed ..." and therefore the organization, i.e. the top management, is basically free to adopt and apply specific methodologies, or not.
- In all standards, the organization is required to "maintain" (e.g. ISO 14001) or "preserve" (e.g. ISO 45001) documented information on the risks and opportunities that need to be addressed.
- The Appendices to the standards themselves do not provide concrete indications of the methodologies to be adopted since they directly refer to the ISO 31000 standard on risk management and related documents (as ISO/IEC 31010, which contains specific indications about methodologies and tools able to support a risk management framework or part of it, as, for example, the risk assessment step). No methodologies are mandatory, since the method, the eventual support tool, the approach (qualitative, quantitative, or mixed), the documentation, and the detail of the risk assessment should be defined considering any eventual regulation, the internal and external context, the competencies, the nature and detail of available data, the results of real incidents and near-misses, and so forth.

According to the third bullet point:

- ISO 9001 in Section A.4, Risk-Based Thinking, indicates that "... there are no requirements that require formal risk management methods or a documented risk management process....";
- ISO 14001 in Section A.6.1.1, General, indicates that "... there are no formal risk management requirements or documented risk management process....";
- ISO 45001 under Section A.6.2.2.2 OSH risk assessment and other OSH management system risks indicates that "... an organization may use different methods to assess OSH risks as part of its overall strategy to address different hazards or activities....".

From this, it would seem that it is possible to deal with risks and opportunities with any approach or even without a structured analytical approach. As anticipated, the risk approach should be defined according to a number of factors and in any case it should satisfy the requirements given by ISO 31000; effective risk management should be integrated, structured and comprehensive, customized, inclusive, dynamic and based on the best available information, coherent with human and cultural factors, and continuously improved. Nonetheless, the rules themselves require the organization to investigate the subject of risk management, based on the complexity of its activities, the context in which it operates, and the level of maturity of the company management system and to manage it with instruments commensurate with the risks.

Also in this case, the only indication is that the instrument, managerial or analytical, must be commensurate with the risks, leaving the organization free to choose, and the best reference is ISO/IEC 31010, which suggests a number of methods (describing both strengths and limitations). The risk-based thinking approach, underlying all the management systems, requires the evaluation of the influence the absence of management tools has on the achievement of objectives; it is therefore natural to look for an analytical tool for risk management, in order to limit the negative influence of its absence and evaluate objectively whether it is commensurate with the risks themselves.

A careful reading of the standards makes it possible to identify more detailed indications as to how any instruments to be used for risk management could, or should, be structured:

- ISO 9001 in Section A.4, Risk-based Thinking, indicates that "... organizations can decide whether or not to develop a more extensive risk management methodology than required ..." by the standard itself, for example "... through the application of other guides or other standards ..." (such as ISO 31000, Risk Management).
- ISO 14001 in Section A.6.1.1, General, indicates that "... the risks and opportunities related to environmental aspects can be determined as part of the assessment of significance ..." and that although it is up to the organization to select the method it uses to determine its risks and opportunities, the method selected "... may involve a simple qualitative process or a complete quantitative evaluation according to the context in which it operates. ...".
- ISO 45001 in Section A.6.2.2, OSH Risk Assessment and Other OSH Management System Risks, indicates that "... the method and complexity of the assessment (OSH risks) do not depend on the size of the organization but on the hazards associated with the organization's activities. ...".

Additionally:

- ISO 9001 in Section 6.1.2 states that "... actions taken to address risks must be proportionate to the potential impact on the compliance of products and services....".
- ISO 14001 in Section 6.1.2, Environmental Aspects, indicates that "... the organization shall determine those aspects that have or may have a significant environmental impact ..." using "... criteria established. ...".
- ISO 45001 in Section 6.1.1.1, General, requires that risks should be determined in order to "... prevent or reduce undesirable effects. ...".

All these principles lead to meeting the requirements of the standards through an analytical approach to risk management that starts from the definition of risk acceptability criteria and the identification of objective analytical tools that allow concrete demonstration of the achievement of the organization's strategic objectives. Valid help for the organization can be found in the framework proposed by ISO 31000, *Risk management – Guidelines* with clause 5 and in application guide ISO 31010, *Risk management – Risk assessment techniques*, which provides a complete overview of the main and most widely used analytical techniques for risk assessment as well as concrete indications for the choice of the most suitable technique (clause 1.1, Scope: "This International Standard is a supporting standard for ISO 31000 and provides guidance on selection and application of systematic techniques for risk assessment").

Barrier-based risk management methods (such as Bow-Tie and LOPA) as well as investigation methods (such as barrier failure analysis), given an initial hazard identification

(HAZOP/HAZID/HAZAN or structured brainstorming or even preliminary hazard analysis), are a suitable approach to implement the requirements of management systems since they operate on basic elements defining risks: possible hazards, threats, top events, associated impacts, and preventive and protective controls (or barriers, or independent protection layers). Furthermore, periodic risk monitoring could be associated with the status of the controls, as the investigation of the root causes of a (real) deviation from intended conditions could be associated with the failure evidences of one or more barriers. This allows risk management, over time, the ability to take into account human factors (as barriers, threats, escalation factors and vulnerable targets given an exposure level, i.e. the condition of being unprotected from hazards, thus leading to risk), and the chance to conduct qualitative and/or quantitative risk assesssment and modify the risk register on the basis of the results of the management of change (MOC) process. Such implementations are able to raise the concept of maturity model of the system considering the risks and their modification in terms of RRFs associated to the control measures.

Irrespective of the actual method used it is important to recognize human and organizational factors, since often investigations reveal that these factors (including individual factors, working environment, organizational factors and physical factors) play a fundamental role in the origin, the development and also the outcome of events.

Also, a risk model can be built with the aforementioned methods regardless of the type: with a consistent single approach it is possible to assess strategic risks (they can have an impact on the organization's ability to achieve its overall objectives and goal), compliance risks (they refer to the organization's exposure to legal penalties and economic losses as a result of non-compliance with applicable laws, regulations and even internal policies) and operational risk (they refer to losses resulting from inadequate procedures, policies, systems, and processes). This inner connection among barrier-based methods and risk management elements allow the organization to have comparable and reproducible results to be discussed with operators, to be illustrated to the stakeholders and to be demonstrated to authorities having jurisdiction and/or third parties (as certification bodies). Comparable results is a key element for prioritization of risks: the organization, given limited resources, needs to prioritize the risk treatment in a way that it considers whether the impact of risks is low or high. This prioritization activity compares scenarios while using multiple criteria (including cost-benefit analysis, feasibility, regulation constraints, level of concern of stakeholders, etc.). Bow-Tie, supported by a quantified LOPA approach, could help in comparing different strategies (different pools and combinations of barriers) and ante, post-modification situations.

Since every management system operation requires the definition of specific roles and responsibilities along with knowledge management activities and competence and training, barrier-based method notation could be easily employed to increase risk awareness and behavioural skills of the stakeholders at various level. The appropriate involvement of people, whose competencies are being developed as part of the training process (educational process aiming to develop knowledge, skills and behaviour in the specific management system domain), may result in them feeling a greater sense of ownership of the process and they will assume more responsibilities. In some cases Bow-Tie diagrams and BFA schemes are used to train people in tabletop exercises: this also guarantees the participation of people with different training levels and different competencies to risk review activities, increasing communication (internal and external) and awareness, and even to comply with specific legal requirements (e.g. safety risks communication, environmental policies, food quality inspections).

Given this, it appears clear that simplicity of such methods could better comply with the documentation requirements of the management systems: if documentation is not mandatory in extension (there is no specific requirement on how to document processes and operational measures and control but documented information is highly valued) it should be available and suitable for use, where and when it is needed. If documents embrace the risk concepts they could be reduced to a minimum and the organization could easily address the following activities:

- Distribution, access, retrieval and use;
- Storage and preservation;
- Control of changes (according to the MOC process);
- Retention and disposition (according to the risk life cycle in the risk register).

In this way the document life cycle aligns with the risk life-cycle described in ISO 31000 with a strong emphasis on the risk-based approach of the latest edition of the ISO standards.

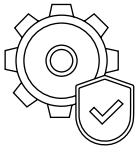
Risk assessment and its documention become the input element for a series of other documents/processes:

- An emergency and response plan should be prepared against the scenarios defined in the risk assessment phase and periodic drills should validate the PFD of the mitigative barriers that are resources for the emergency response.
- Procurement activities related to critical elements (preventive and mitigation barriers) should comply with performance standards that maintain the PFD declared in the risk assessment.
- Competency and training of contractors with a critical role in the risk diagram are fundamental.

All the processes should be defined and assessed in terms of risk, but also monitored and reviewed over time. These pillars of the management systems could be achieved linking KPIs to barriers and to pathways from threats to impacts, as well as linking root cause analysis results to barriers to identify weak points in the processes and activate preventive/corrective actions and general improvement of the management system in the spirit of the PDCA global framework, to be discussed in the periodic management review, in which, via a risk-based decision process, it is possible to define any eventual needs to mitigate the risk of deviation from defined processes goals and strategic objectives of the entire organization via a specific action plan, whose results could be simulated via a generation of specific diagrams to compare actual and future configurations of the controls in the overall picture, along with the associated RRFs, resources, responsible people and documents. Improvement of the management system does not only rely on documentation update but also in factors of change consideration (specifically those affecting the risk register and the risk assessment). Continuous improvement leads to:

- Better process performance, enhanced organizational reputation and increased stakeholder satisfaction;
- A greater ability to react to risks (even new and emerging);
- Ensuring that people acquire the required competency level;
- Recognition and acknowledgement of performance improvements.

1.7.2 Industrial Safety (Major Accidents)



Barrier-based safety management systems are now widely adopted because of the advantages of their barrier-based perspective. Among the different methods that are available to implement them, the Bow-Tie is one of the most recognized ones. Leveraging its persuasive visual communication, it allows all the stakeholders of the risk management process to have, in a single shot, the complex picture of the relations linking threats, preventive barriers, top events, mitigative barriers, consequences, and escalation factors. There is a strong relationship between the four pillars of process safety management systems (commitment to process safety, understanding hazards and risks, risk management, and learning and improvement), the standard steps of the Deming safety life cycle and the Bow-Ties, also making use of the first official guidelines by AIChE CCPS. The payoff is tremendous: risk assessments come to life. Instead of being forgotten and archived, risk assessments are used because they are relevant in day-to-day operation. Thanks to the "Work Bow-Tie," operators know exactly the risks they are going to face when performing ordinary or extraordinary maintenance, also helping significantly in the evaluation of interferential risks and work-permit management. Furthermore, the aggregation of various data sources allows a level of understanding and insight into risks, which is unprecedented in risk management until now. The "Do" phase is followed by the "Check" one. This is when the organization looks for occasions for improvement: internal audits and incident analysis are part of this step. Their results are enhanced and appreciated thanks to the Bow-Tie approach, because they are now performed from a barrier-based perspective, meaning that the barriers are monitored in their effectiveness (audits) and eventual failings (incident analysis). This results in positive feedback for the "Plan" step of risk assessment that is now adjusted with the data coming from the real operative experience of the organization. Finally, audit recommendations, safety observations and incident actions are then evaluated and implemented during the "Act" phase, and the risk assessment is once again updated accordingly. The EU Directive on Major Accidents Prevention (also known as the Seveso Directive), EU Directive 2012/18/EU dated 4 July 2012, request for operators to have a specific major accident prevention policy (MAPP) supported by an appropriate safety management system (SMS) for controlling major accident hazards. This SMS has specific pillars, very similar to those of the OSHA process safety model: organization and personnel, identification and evaluation of major hazards, operational control, management of change, emergency planning, performance monitoring, audit and review activities. In order to demonstrate that everything necessary has been done to prevent major accidents, and to prepare emergency plans and response measures, the operator should provide the competent authority with information in the form of a safety report (updated on a periodic basis, usually every five years). This safety report should contain details of the plant, dangerous chemicals and their quantity, possible major accident scenarios and risk assessment, prevention and intervention measures (controls or barriers), and the SMS in place in

order to prevent and reduce the risk of major accidents. Minimum data to be considered include, in a risk management approach: identification and accidental risk analysis and prevention method, major accident scenarios and their likelihood and causes (operational, external and domino, Na-Tech, cyber) along with the consequences, review of past accidents and incidents (including near-misses), controls in place (preventive and protection measures), and emergency plan. Authorities having jurisdiction should verify that the risk-reducing factors (RRFs) declared in the safety report (by the plant owner) are valid and maintained during the life cycle of the plant, by the support of the safety management system put in place. Declared PFD of the barriers shouldn't exceed data used in the risk assessment. Risk management workflow is completely inspected with two different audits: on the safety report content (assumptions, results, risk mitigation plans) and on the SMS in place (is the major accident risk from the safety report kept under control over time?). Since risk management also fails when a modification is put in place, MOC should be considered an ineludible part of the management system. Authorities should verify that the MOC process is included and actuated for each plant modification (even temporary) and that the plant life cycle coincides with the control measures (barriers) life cycles. In their safety report plant operators should answer three specific questions:

1) Do we understand what can go wrong?
2) Do we know what our systems are to prevent this happening?
3) Do we have information to assure us they are working effectively?

These answers are strictly related to threats and barriers in place to control and possibly avoid an impact or loss to vulnerable targets (people, environment and assets in Seveso plants) and the combination of the safety report with SMS is a good example of applied barrier thinking and risk management over time. In fact, an effective way to obtain a low probability of a major accident occurring is to use a system composed of multiple levels of protection, also called "defense in depth" and well represented with the Swiss Cheese Model by Reason, applied, as exemplification, to a major industrial event in Figure 55.

The LOPA approach is a quite common technique used during scenario screening. LOPA allows the assessment of the IPLs for each "threat-impact" pair that define a scenario. IPLs considered are those that control the deviation from the normal behaviour of a process value that is governed by the process control layer: process alarms, trip level alarms, emergency shutdown systems and safety instrumented functions, mechanical devices (relief

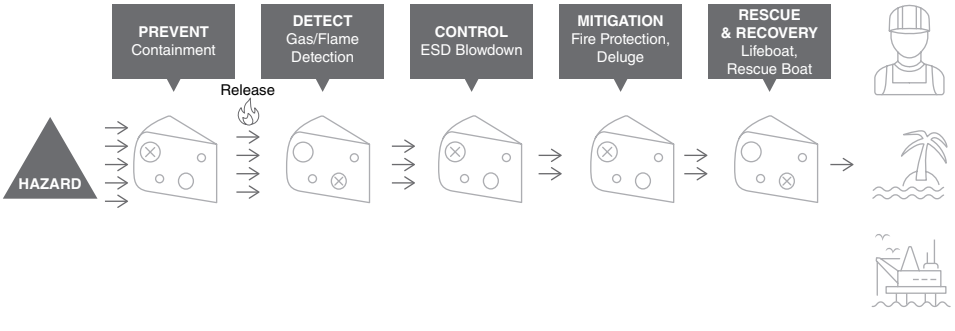
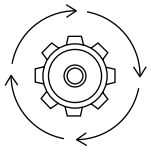


Figure 55 Swiss Cheese Model applied to a major industrial event.

valves, rupture disks), passive protection layers (dikes), emergency response layers (emergency plan, fire protection systems, etc.). A safety management system strategic goal is to keep barriers in place over time. Barriers could fail and the human factor plays a fundamental role, and each barrier could be assigned a specific PFD depending on a condition of the barrier. Human response to alarm, for example, is the first line of defence: it can be linked to a RRF of 10 (PFD = 0,1) in case specific conditions are verified for an effective control room operator response: written procedures are available, an operator is present 24 hours a day, and the operator has an indication of the problem, has enough time to act, andhas received proper information, education, and training on a periodic base.

The plant owner should demonstrate the availability of barriers and associated RRFs, as they have been identified and declared in the risk assessment of the safety report; the owner could use recognized and generally accepted good engineering practices (RAGAGEP) standards. Barriers, during inspections by the authorities, are verified in terms of condition and associated (declared) RRF/PFD, since these data come from a performance- and risk-based approach (analysis, design and operation), eventually integrated with the life cycle of RAGAGEP requirements in the framework of a specific organization culture, as recommended by the fundamental principles of ISO 31000.

1.7.3 Functional Safety and RAGAGEP Standards



When it comes to process safety, most companies focus on the functional safety life cycle and compliance with the international standard IEC61511, "Functional safety: safety instrumented system for the process industry sector." The functional safety life cycle (SLC) provides the foundation for building a set of processes and procedures that support risk reduction and risk management, as defined within the standard itself. If followed correctly, the SLC provides a consistent methodology for achieving repeatable results, based upon a set of performance targets to manage and mitigate process risk within acceptable boundaries. The SLC can be applied to any hazardous process, whether it be chemical, petro-chemical, oil & gas, pharmaceutical, food and beverage and/or machine applications. A key objective of IEC61511 is the definition of the safety integrity level (SIL), 1/PFD, to be associated to critical safety instrumented functions (SIFs) employed to mitigate the industrial risks together with the other IPLs in place. Examples of SIFs are alarm systems, emergency shutdown systems, fire and gas detection systems, interlocks, andso on. Risk reduction factors needed to achieve an acceptable risk (with an ALARP approach) should be maintained over time considering architectural redundancy, inspection and test intervals, proof tests, maintenance operations, and so on. Among the methods suggested, implementing the SLC Bow-Ties and LOPA assessments plays a fundamental role as risk control focused methods. However, with the advent of the industrial internet of things (IIOT) and the growing use of wireless technologies, it is becoming more important to consider cybersecurity and the consequences of control and safety systems being compromised due to a cyber-related incident.

Similarly, if there is no defined alarm philosophy and rationalization of alarms, operators can miss vital alarms and lose valuable time in being able to respond to an incident due to the volume of alarms being generated. Accidents, such as the Buncefield and Texas City explosions, highlighted the problem, with operators being confused by too many alarms. Since the standards for functional safety (IEC 61511), alarm management (IEC 62682) and cybersecurity (IEC 62443) all follow a similar phased lifecycle (PDCA), it makes sense to consider all three together when it comes to process safety. As such, an integrated life cycle approach will help in reducing overall operational costs via increased efficiencies. The success of this implementation relates directly to the company's maturity and culture when it comes to adopting industry best practices. Synergistic benefits can be gained by considering all three together, when combined with the company's maturity level, that is strictly related to the quality of the culture and of the risk management process of the company. In the framework of an advanced maturity model in risk management practices, common elements of life cycles (usually built on a three-phase approach Analysis-Design-Operation similar to the more general PDCA), coupled with requirements of RAGAGEP guidelines could lead to an holistic composition, as described in Figure 56, where alarm management, cybersecurity and the functional safety life cycle are combined to support the plant operator in the management of the industrial risk associated with his plants and assets. In this sense:

1) Adopting RAGAGEP standards is the best way to assure a holistic composition towards an advanced maturity model.
2) Plant life cycle should be verified against the pillars of the SMS.

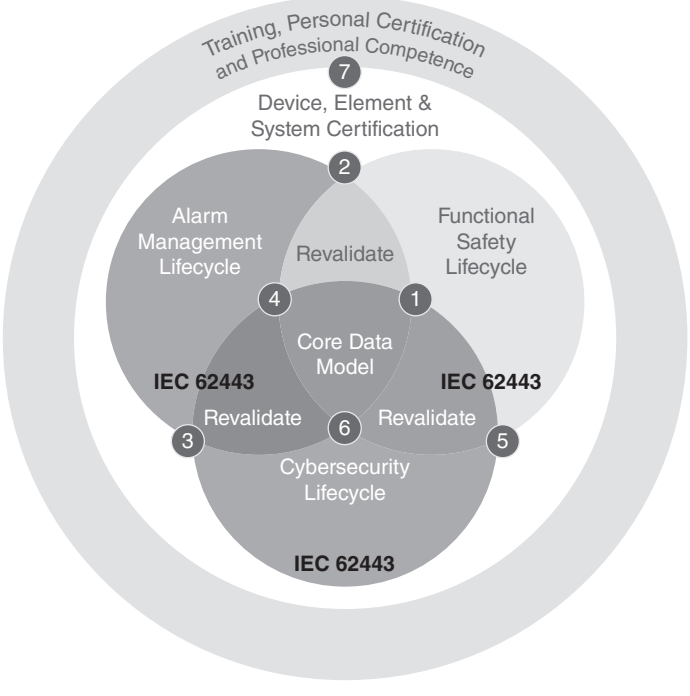
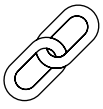


Figure 56 Maturity model. *Source:* Courtesy of EXIDA L.C.C. (USA).

3) Barrier life cycles should comply with the life cycles requested by RAGAGEP standards.
4) Plant owners could take advantage of a single integrated approach to deal with known risks and face emerging risks (e.g. cybersecurity).
5) RAGAGEP standards and supporting methods or tools could demonstrate the results to AHJ: credible, trackable, documented and justified performances in a risk-based framework coherent with ISO 31000 risk management principles.

1.7.4 ISO 55000 (Asset Management and Integrity)



ISO 55000 is an international standard covering management of assets of any kind. Before it, a Publicly Available Specification (PAS 55) was published by the British Standards Institute (BSI) in 2004 for physical assets. This standard focuses on helping the organization develop a proactive life-cycle asset management system. This supports optimization of assets and reduces the overall cost of ownership while helping the organization to meet the necessary performance and safety requirements. An asset management system provides a structured, best-practice approach to managing the life cycle of assets, with:

- Reduced risks associated with ownership of assets, including safety-related risks and business continuity risks;
- Improved quality assurance for customers/regulators, where assets play a key role in the provision and quality of products and services;
- New business acquisition – stakeholders recognize that top management put in place a strategy to ensure that assets meet the necessary safety and performance requirements (including environmental compliance).

This standard complies with the ISO 72 guidelines and justification for the development of management system standards. These guidelines outline the common elements of policies, planning, implementation, operation, performance evaluation, improvement and review by management. It also establishes that the management systems should be developed under the PDCA approach. ISO 55000 highlights that assessing the value of the organization's assets takes risk into consideration (as defined in the ISO 31000 referenced standard). It's important to underscore that ISO 55001 is not a standard on reliability and maintenance management (better described in a number of other documents, guidelines, books, etc.), but that doesn't mean that maintenance and reliability doesn't have an important role in it. Annex A (informative) for example explicitly mentions condition monitoring, life-cycle cost, non-destructive tests, and so on. Asset management, as per ISO 55000, covers the asset's life cycle, which considers all the different life steps of an asset: concept, design, procurement, construction/installation, commissioning (including pre-startup safety reviews), operation, maintenance, decomissioning and final disposition. In all the identified phases, a proper MOC process should be in place and documented.

ISO 55000 is applicable to any industry sector and considers different types of assets: material assets such as infrastructure, plant, equipment, buildings and other tangible objects, but also intangible assets such as good-quality business data, information systems, licenses, and other intangible assets such as brand, reputation, image, and customer loyalty of the organization.

However, physical assets are the lifeblood of all production processes. If a critical asset should fail, it could not only cause a security or environmental problem, but also disrupt business until it is repaired or replaced. By applying the standard, companies can gain a complete view of the integrity of the entire plant by removing the watertight compartmental approaches that exist in many facilities. They can also create a strategic plan for resource utilization and maintenance so that repairs and replacements are scheduled with minimal disruption to production.

It is quite obvious that integrity is a performance of the asset that should be maintained during the lifetime of an asset: in some cases a loss of integrity could result in severe impacts (e.g. loss of containment of vessels operating with a toxic chemical in a chemical facility, loss of stability of a bridge, etc.). Risk assessment plays a fundamental role in asset management in all its components: initial and periodic risk assessment and root cause analysis of real incidents to understand the causal relationship with the controls in place to avoid or mitigate the impact. Also, a single top event (loss of containment or integrity) can be related to threats involving different specific domains such as loss of containment due to overpressure, ageing, or human error. A top event could lead to an impact on several vulnerable receptors (people, environment, or assets due to domino effects). Given this example, it is clear that asset management could gain a serious advantage from a barrier-based approach that, for each control in place, defines failure mechanisms that determine the probability of failure on demand, to be related with the likelihood of the impacts. But, due to the complexity of asset-related threats and their evolution in impacts, the advantage could also be recognized in the ability to consider human factors, design (poor) conditions, time-related mechanisms to be monitored during time (e.g. corrosion, erosion, fatigue, creep, inspections effectiveness, etc.), escalation and contributing factors (as well as seasonal risk) or conditional modifiers (as those used in LOPA), and so forth. This approach, often represented via a fishbone diagram, has been effectively used to describe the portion of an asset management system, integrated with Seveso risk assessement, related to the ageing issues for integrity of vessels and equipment in chemical plants.

1.7.5 ISO 22301 (Business Continuity)

ISO 22301, *Societal security – Business continuity management systems – Requirements*, is an international standard related to business continuity management (BCM), which defines the requirements necessary to plan, establish, implement, and operate a documented management system, and to monitor, maintain, and continuously improve the management

system to protect, reduce the possibility of occurrence, prepare, respond to, and restore destabilizing events for an organization when they occur.

The standard specifies requirements to implement, maintain, and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to, and recover from disruptions when they arise.

The requirements specified in the standard are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size, and nature of the organization.

The extent of application of these requirements depends on the organization's operating environment and complexity.

This document is applicable to all types and sizes of organizations that:

- Implement, maintain and improve a BCMS;
- Seek to ensure conformity with stated business continuity policy;
- Need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption;
- Seek to enhance their resilience through the effective application of the BCMS.

The standard helps organizations to:

- Identify and manage current and future threats to business processes or to the entire organization;
- Adopt a proactive approach to minimize the impact of accidents;
- Keep critical functions active during periods of crisis;
- Minimize downtime during accidents and improve recovery time;
- Demonstrate the company's resilience to customers, suppliers, and requests for quotation.

Therefore there is clearly a link between business continuity issues and risks and a strict correlation among the risk register and the business impact assessment (BIA).

The organization is requested to define, implement, and maintain a formal and documented process for business impact analysis "AND" risk assessment that:

- Establishes the context of the assessment, defines criteria, and evaluates the potential impact of a disruptive incident;
- Takes into account legal and other requirements to which the organization subscribes;
- Includes systematic analysis, prioritization of risk treatments, and their related costs;
- Defines the required output from the business impact analysis and risk assessment, and specifies the requirements for this information to be kept up-to-date and confidential.

The organization, with reference to the risk management system supporting the BCMs, is requested to:

- Identify risks of disruption to the organization's prioritized activities and the processes, systems, information, people, assets, outsource partners and other resources that support them;
- Systematically analyze risk;
- Evaluate which disruption-related risks require treatment;
- Identify treatments commensurate with business continuity objectives and in accordance with the organization's risk appetite.

BCM is a vital process to assure resilience over time: since disruptions could be determined by new and emerging risks it is fundamental to keep in place a dialogue with the risk management process and also learn from experience, even considering soft events, and performance monitoring during real events and drills. A barrier-based approach can induce the assessment of common cause failures that could affect more organization processes or determine the failure of several controls.

In this particular domain field, an easy notation, like the notation used by Bow-Tie/LOPA and by BFA, could be very effective in communicating relationships and describing business continuity procedures and in defining an incident response structure against identified disruptive events, with all the documents, roles and responsibilities associated (these elements guarantee the RRF associated to each control). Results of the assessment can be documented in business continuity plans and exercising and testing plans.

1.7.6 ISO IEC 27001 (Information Security)

ISO/IEC 27001, *Information Technology – Security Techniques – Information Security Management Systems – Requirements*, is an international standard that defines the requirements for setting up and managing an information security management system and includes aspects related to logical, physical and organizational security. Since information is an asset that adds value to the business, and since most information is now stored on computer media, every organization must be able to ensure the security of its data, in a context where the IT risks caused by breaches of security systems are constantly increasing. The objective of the most recent edition of the ISO 27001 standard is precisely to protect data and information from threats of any kind, in order to ensure its integrity, confidentiality and availability, and to provide that the requirements adopt an adequate information security management system aimed at a proper management of sensitive company data. The standard is applicable to companies operating in most commercial and industrial sectors, such as finance and insurance, telecommunications, services, transport, and government sectors. The approach of the ISO/IEC 27001 standard is consistent with the general framework ISO 31000 on risk management, based on the process approach, structured in safety policy, identification, risk analysis, risk assessment and treatment, risk review and re-evaluation, the PDCA model, use of procedures and tools such as internal audits, nonconformities, corrective and preventive actions, and surveillance, with a view to continuous improvement.

In the design phase of the information security stategy, ISO 27001 requires a risk assessment, which can be schematized in the steps well described in the ISO 31000 standard:

- Risk identification;
- Analysis and evaluation;
- Selection of control objectives and control activities for risk management;

- Assumption of residual risk by management (calculated via an ALARP approach);
- Definition of the Statement of Applicability.

The last point specifies the control objectives adopted and the controls implemented by the organization with respect to a list of control objectives provided by the standard itself. Fundamental to the standard is the informative Annex A, *Control objectives and controls*, which contains the 133 controls with which the organization that intends to apply the standard must comply. They range from security policy and organization to asset management and human resources security, from physical and environmental security to communications and operational management, from physical and logical access control to incident monitoring and handling (related to information security). Management of business continuity and regulatory compliance completes the list of control objectives. The organization must justify which of these controls are not applicable within its ISMS, for example, an organization that does not implement e-commerce within its ISMS may declare as not applicable the controls 1-2-3 of A.10.9 that relate to e-commerce activities.

1.7.7 ISO 19011 (Audit)

ISO 19011 provides guidance on the audit of management systems, including the principles of audit activity, management of audit programs, and the conduct of management systems audits, as well as a guide for assessing the skills of the people involved in the audit process. These activities include the person(s) managing the audit program, auditors, and audit teams. The standard is applicable to any organization that needs to plan and conduct internal or external management system audits or to manage an audit program. Since the publication of the latest edition of this document, a number of new management system standards, many of which have a common structure, identical basic requirements, common terms, and fundamental definitions. It follows the need to consider a more extensive approach for the audit of management systems, as well as to provide a more general guide. The biggest differences compared to the previous edition are:

- The addition of the risk-based approach in the principles audit;
- The extension of the program management guide;
- Audits, including the risk of the audit program;
- The extension of the audit conduct guide, in particular the section on audit planning;
- The extension of the general competence requirements of auditors;
- The arrangement of terminology;
- The extension of Annex A to offer guidance on the (new) audit concepts, such as context of the organization, leadership and commitment, virtual audits, legislative compliance, and the supply chain.

The organization should conduct internal audits at planned intervals to provide information on whether the management system(s) in place conforms to the organization's own

requirements and the requirements of the reference standard and to provide information on whether the system is effectively implemented and maintained over time.

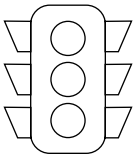
In this sense the organization should:

- Plan, establish, implement, and maintain an audit programme(s), including frequency, methods, responsibilities, planning requirements, and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits.
- Define the audit criteria and scope for each audit.
- Select auditors and conduct audits to ensure objectivity and the impartiality of the audit process.
- Ensure that the results of the audits are reported to relevant management.
- Retain documented information as evidence of the implementation of the audit programme and the audit results.

The risk-based approach should influence the planning, conducting, and reporting of audits, in order to ensure that the latter are focused on issues that are significant for the audit client and to achieve the objectives of the audit program. One of the main goals of an audit is the maturity model of the organization in the risk management workflow, especially in the risk assessment steps and in the following activity to define actions, plans, and priorities. Since audit is a fundamental activity that guarantees the monitoring and review of the maturity model, it should be conducted in a way that critical elements of the management systems (and related recordings) are verified. In a risk-based approach to management systems for each scenario, the organization should identify control elements (preventive and mitigative barriers). During audit the inspection team should verify the controls identified by the risk assessment: presence and correct operation (as intended). They also should verify any eventual records related with near-misses and incidents in order to associate the root cause analysis results with the affected barriers and following decisions to avoid a recurrence. A risk-based audit is quite different from a traditional audit, the latter aimed to the exclusive and simple verification of the satisfaction of precise and predefined requirements. A risk-based audit is more complex since with document sampling and discussions the inspection team should evaluate the entire maturity model of the audited management system/systems and the underlying risk management common framework. This requirement calls for a different competency level of the auditors, who should also be proficient in risk management principles. While traditional audits were characterized by a single-focus approach on a specific aspect (e.g. training and competence, maintenance, work procedures, time programming, management review), risk-based audits are based on performance and are focused on controls or barriers identified as critical (and eventually recorded in a specific register) and on their failure mechanisms, since PFD is strictly connected with the sum of the causes (internal, external, common, etc.) that can determine partial or total failure, considering also human factors. Considering the results of a fire risk assessment, the internal emergency plan is a critical protection barrier since it helps in reducing the impact of a fire scenario to people, assets, and the organization's business continuity. This barrier could fail due to different causes, related to different aspects: the emergency plan is not available (work procedures), the emergency team doesn't know the plan (training), periodic drills are not organized (time programming), the plan is

not updated (maintenance), the operator does not have the skills or time to put in place emergency procedures described in the plan (human factor), or the plan is available but its content is wrong (risk assessment). Given this example, the audit process is an opportunity to review the risk management process focusing on the elements that have been identified by risk assessment as critical elements for the organization.

1.7.8 ISO 39001 (Road Traffic Safety)



Road traffic safety is a global and well known problem. Road accidents and accidents at work are closely related: in Italy more than half of the accidents at work recorded by the Italian National Institute for Workplace Incidents Insurance (INAIL) statistics in 2011 (436 deaths, equal to 50.6% of the total) belong to the road traffic categories or ongoing travels, with or without means of transport. Alongside the growing attention to health and safety issues in the workplace, which has seen an increase in laws and decrees in recent years, with the increase in road traffic there has also been a growing awareness of road safety, both on the part of institutions and road users. ISO 39001 certification provides a global approach to road safety. ISO 39001 defines the necessary and useful elements for proper management of good practices aimed at road safety, with a specific focus on the actions taken and the expected results achieved with a view to improving prevention. The road traffic safety management system can be integrated or made compatible with all other management systems. The certification against ISO 39001 consists of assessing the dynamics of the organization's processes with respect to the transport system and road safety, verifying the acceptability of risk exposure and analyzing the actions taken in order to reduce both the probability of incurring a road accident and the severity of the same. Safety is strictly related to organization and its context; a special case are organizations where transportation is a usual activity of core business processes. The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its road traffic safety management system. In particular, each organization should identify its role in the road traffic system, identify the processes, associated activities and functions of the organization that can have an impact on road safety and also determine the sequence and interaction of these processes, activities and functions. The organization should prepare and update a risk assessment with the actions needed to prevent, or reduce, undesired impacts. A fundamental role in this initial risk assessment process is the identification of risk exposure factors, risk outcomes (consequences in terms of fatalities and injuries), and barriers available to prevent and mitigate the consequences such as:

- Road design and safe speed, especially considering separation (oncoming traffic and vulnerable road users), side areas and intersection design;
- Use of appropriate roads, depending on vehicle type, user, type of cargo and equipment;

- Use of personal safety equipment, especially considering seat belts, child restraints, bicycle and motorcycle helmets, and the means to see and be seen;
- Using safe driving speed, also considering vehicle type, traffic and weather conditions;
- Fitness of drivers, especially considering fatigue, distraction, alcohol and drugs;
- Safe journey planning, including consideration of the need to travel, the amount and mode of travel and choice of route, vehicle and driver;
- Safety of vehicles, especially considering occupant protection, protection of other road users (vulnerable as well as other vehicle occupants), road traffic crash avoidance and mitigation, roadworthiness, vehicle load capacity and securing of loads in and on the vehicle;
- Appropriate authorization to drive or ride the class of vehicles being driven or ridden;
- Removal of unfit vehicles and drivers or riders from the road network;
- Post-crash response and first aid, emergency preparedness, and post-crash recovery and rehabilitation.

Controls should be used in the risk assessment and this initial activity should be completed by a specific training and awareness program and by an incident investigation of negative impacts (road traffic crashes and incidents). Investigations should understand missing, poor, or non-effective controls as well as determine the underlying factors that the organization can control and/or influence that might be causing or contributing to the occurrence of those incidents.

1.7.9 ISO 19600 (Compliance Management Systems)

Organizations that aim to be successful in the long term need to maintain a culture of integrity and compliance, and to consider the needs and expectations of stakeholders. Integrity and compliance are therefore not only the basis, but also an opportunity, for a successful and sustainable organization. Compliance is an outcome of an organization meeting its obligations, and is made sustainable by embedding it in the culture of the organization and in the behaviour and attitude of the people working for it. While maintaining its independence, it is preferable for compliance management to be integrated with the organization's financial, risk, quality, environmental, and health and safety management processes and its operational requirements and procedures. An effective, organization-wide compliance management system enables an organization to demonstrate its commitment to compliance with relevant laws, including legislative requirements, industry codes, and organizational standards, as well as standards of good corporate governance, best practices, ethics, and community expectations. Embedding compliance in the behaviour of the people working for an organization depends above all on leadership at all levels and clear values of an organization, as well as an acknowledgement and implementation of measures to promote compliant behaviour. Non-compliance risks could pose a number

of consequences to business continuity, to the organization leadership on safety (e.g. safety protection measures are not compliant with specific laws). Compliance with applicable rules, laws and regulations, but also with standards in general terms, assure risk reduction; therefore, compliance risk should be considered in the assessement of failure mechanisms of barriers, including the human factor (e.g. failure in period training of emergency team staff could result in a fine but also in a reduced performance of the emergency team during a fire). Compliance risk can be characterized by the likelihood of occurrence and the consequences of non-compliance with the organization's compliance obligations (including mandatory and volountary commitments).