AN INTRODUCTION TO RISK CONSIDERATION

Introduction

This cookbook aims at recalling basic concepts and providing simple tools and possibilities of applying the "considering of risks and opportunities" in the framework of the ISO / IEC 17025:2017.

The risk-based approach and the awareness of risks is accentuated in the new version of the standard and a risk-based thinking approach and process design in the laboratory is promoted; although ISO 9001:2015 and ISO/IEC 17025:2017 do not stipulate a complete risk management system (RMS), for example conforming to the requirements of ISO 31000.

Dealing with risks and opportunities in the laboratory is not a novelty. The previous version of ISO/IEC 17025 already used the term risk in several chapters, particularly in the context of corrective and preventive actions but also associated with validation of methods and the introduction of the concept of uncertainty of measurement. If a laboratory knows its risks, it has the capability to assess/prioritize them and is also informed about the consequences. It will be easier to make plans how to come up with risks and their effects. Recognizing mistakes or nonconformities at an earlier stage gives the laboratory the opportunity to react early. Financial penalties or other heavy losses might be averted. The main goal of this is not minimizing any risks, but in fact optimizing the laboratory profile of risks and opportunities determined by the laboratory strategy.

The requirements of ISO/IEC 17025:2017

The international standard ISO/IEC 17025:2017 states in its introduction:
This document requires the laboratory to plan and implement actions to address risks and opportunities. Addressing both risks and opportunities establishes a basis for increasing the effectiveness of the management system, achieving improved results and preventing negative effects. The laboratory is responsible for deciding which risks and opportunities need to be addressed.

The laboratory is responsible for deciding which risks and opportunities need to be addressed. The accreditation body, however, assesses whether the laboratory has established appropriate actions for dealing with risks and opportunities in accredited laboratories.

The standard explicitly refers to the term risk in:

- Foreword,
- Introduction,
- Clause 4.1.4 and 4.1.5 on impartiality,
- Clause 7.8.6.1 considering the risk in terms of decision rules used in reports,
- Clause 7.10.1 related to management of nonconforming work,
- Clause 8.5 on actions to be implemented to address risks and opportunities,
- Clause 8.6 on improvement
- Clause 8.7 on corrective action
- Clause 8.9 on management reviews.

Clause 8.5 “Actions to address risks and opportunities” sets minimum requirements for laboratories which shall be considered. The exploitation of improvement potentials should always be aligned with the aim and purpose of laboratory activities.

Mind the Clause 8.5.2 NOTE:

> ***"Although this document specifies that the organization plans actions to address risks, there is no requirement for formal methods for risk management or a documented risk management process. Laboratories can decide whether or not to develop a more extensive risk management methodology than is required by this document, e.g., through the application of other guidance or standards."***

Conversely, a minimum of formalism allows the laboratory to capitalize on the approach and motivate more effectively the deployment of provisions, sometimes perceived only as constraints.
Some words may encourage the consideration of related risks to help the implementation of requirements.

Examples:

- sufficient (clauses 7.2.1.2, 7.5.1),
- suitable (clauses 6.3.1, 8.3.2),
- prevent (clauses 5.6.c, 6.3.4, 6.4.3, 6.4.9, 6.4.12, 7.7.3, 8.3.2, 8.5.1.c),
- ensure (clauses 5.5.c,)
- critical (clauses 7.6.3, 7.8.2.1).

Terms and definitions related to risks.
Various definitions of the term "risk" can be found in normative documents. The following definitions are freely derived from them.

- **Risk:** what makes achieving an objective uncertain.
- **Level of Risk:** an expression of the importance of the risk taking into account the consequences and the likelihood of situations.
- **Risk evaluation:** comparison of the level of risk with an acceptance criterion
- **Risk treatment:** Many options are possible and can be combined: avoiding the risk, taking the risk to seize an opportunity, eliminating the source of risk, changing the likelihood of occurrence or consequences, sharing risk or accept risk as it is and inform on it.
- **Residual risk:** Risk remaining after risk treatment.
- **Opportunity:** an event with potential positive consequences for the organization.

How to assess risks in a laboratory?

To identify risks, it is useful to consider both the internal context of the organization and its external context (risks related to the customers of the laboratory, its suppliers, and also to final client and other stakeholders).

Risk identification methods range from common sense and brainstorming, the use of pre-established lists for a professional sector, to the use of standards setting good practices.

For example:

The SWOT analysis is a process that identifies an organization's strengths, weaknesses, opportunities and threats. It can be used for brainstorming.

List of **S**trengths (internal positive factors)	List of **W**eaknesses (internal negative factors)
List of **O**pportunities (external positive factors)	List of **T**hreats (external negative factors)

The 4 boxes are filled with the relevant information ranked by decreasing importance.

For example:

Guidelines on risk management give various approaches.

Referring to the clauses previously mentioned in ISO 17025, the risk assessment can be approached by answering the following questions:

- What can happen and why (by risk identification)?
- What are the consequences?
- What is the probability of their future occurrence?
- Are there any factors that mitigate the consequence of the risk or that reduce the probability of the risk?

To properly address risk in the laboratory, it is necessary to start with a thorough analysis of the risks that a laboratory might face. The aim should be to prevent weaknesses in the laboratory activities.

The influences and causes are analyzed based on the risk scenario. This assessment can either lead to the initiation of measures or the acceptance of the risk as such. If measures are taken, their effectiveness shall also be examined. It is possible that a risk is deemed acceptable without any mitigation mainly to pursue an opportunity.

The risk scenario is often easy to define. Considerations similar to the case of "preventive measures" can be taken.

Furthermore, a laboratory may decide to implement a comprehensive risk and opportunity management system as defined in ISO 31000. For more details see annex A.

When are risk assessments carried out?
Answer: Whenever it is necessary (e.g., customer requirements or ISO/IEC 17025) or if it helps to achieve the objectives of the management system. This may be regular or occasional in case of abnormalities or changes in the laboratory procedures.

In fact, the laboratory should face risks (e.g., to its existence, to its impartiality, to the validity of its results, etc.) that may lead to failure, loss, damage, or others and counteract them in an appropriate manner by establishing either an RMS or using other measures. (*See Annex A for examples of "Who does what", "Risk Categories" and "Risk Registration Form". These measures exceed the requirement of ISO 17025: 2017 but could be useful in creating a comprehensive risk management system*).

Clause 4.1.4 of ISO/IEC 17025 requires identifying risks to impartiality on an on-going basis. For example, for some personnel on-going handling of risks can be ensured through a self-declaration of conflict of interest yearly reviewed with obligation of update if a new situation affecting impartiality occurs.

In analyzing the risk of impartiality, it is suggested to consider the entire process, intended both as the performance of operational activities and as a management system and organizational

context.

This analysis must be updated continuously, examining the context, the interested parties and all the organizational and operational elements of the Laboratory, with the aim of identifying both the risk factors (potential or real) and the internal and / or external functions, more directly involved.

It is necessary to check the following aspects:

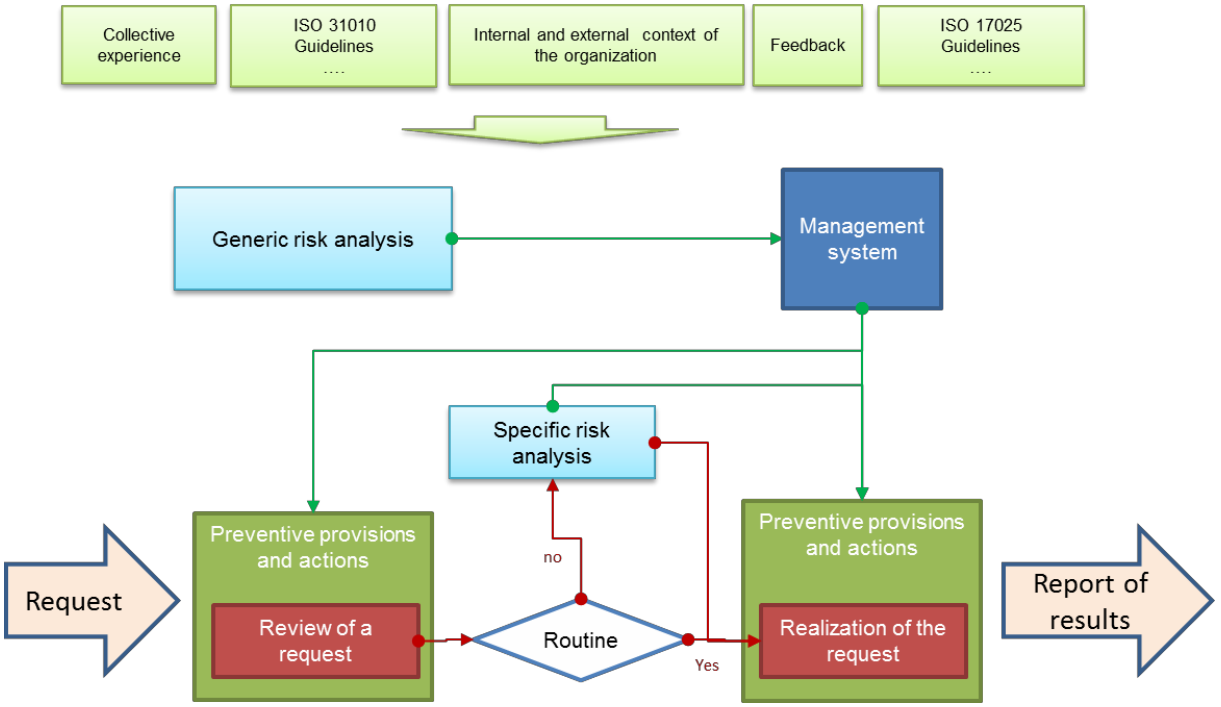
- ownership and management
- type of services offered and shared resources
- availability and use of financial resources
- management of internal and external human resources
- contracts
- responsibilities and methods of carrying out the activities of execution, control, revision, approval and signature of the test certificates.

The criticality of the risks highlighted is then assessed and the measures to be adopted to prevent, eliminate, or minimize their effects are defined.

Application in a more general context

The organization according to its needs may have a more or less explicit policy of taking into account the risks. This can include management of activities, financial management, safety, etc. The mechanisms for updating information can be more or less developed, ranging from risk management to mere reaction to failures.

The following example shows a mechanism for the construction of preventive measures based on risk analyzes. Many other approaches are possible.



ANNEX A - EXAMPLE OF A COMPREHENSIVE RISK MANAGEMENT SYSTEM

To be able to carry out an assessment, the impact, the probability of occurrence and the probability of a risk being quickly discovered (detectability) should be assessed.

It is helpful to share a scale of value within the organization, whatever is the representation: quantitative or qualitative, represented in tables, in graphs etc.

A risk assessment can be conducted for example by a four-stage quotation system.

The following table provides an indication for assigning the probability levels of a risky event and its impact on business programs:

QUALITATIVE MEASURE OF RISK PROBABILITY (P)		
LEVEL		
1	LOW	Extremely unlikely, it could happen but only in exceptional circumstances. It has never happened before.
2	MEDIUM-LOW	Unlikely, but possible, to happen or happen again. Previously, however, it occurred rarely.
4	MEDIUM-HIGH	It will likely happen or happen again. Previously, it has already occurred.
5	HIGH	Continuous exposure to risk. Previously, it always occurred frequently and regularly.
QUALITATIVE MEASURE OF RISK IMPACT (I)		
LEVEL		
1	LOW	None, or only minimal impact, on the objectives and timing of the planned activities.
2	MEDIUM-LOW	Tolerable costs. Limited impact on objectives and timing of planned activities.
4	MEDIUM-HIGH	Relevant financial losses. It will likely affect the achievement of some program goal.
5	HIGH	Critical financial losses. It will likely affect the achievement of many of the program objectives, if not the success of the program itself.

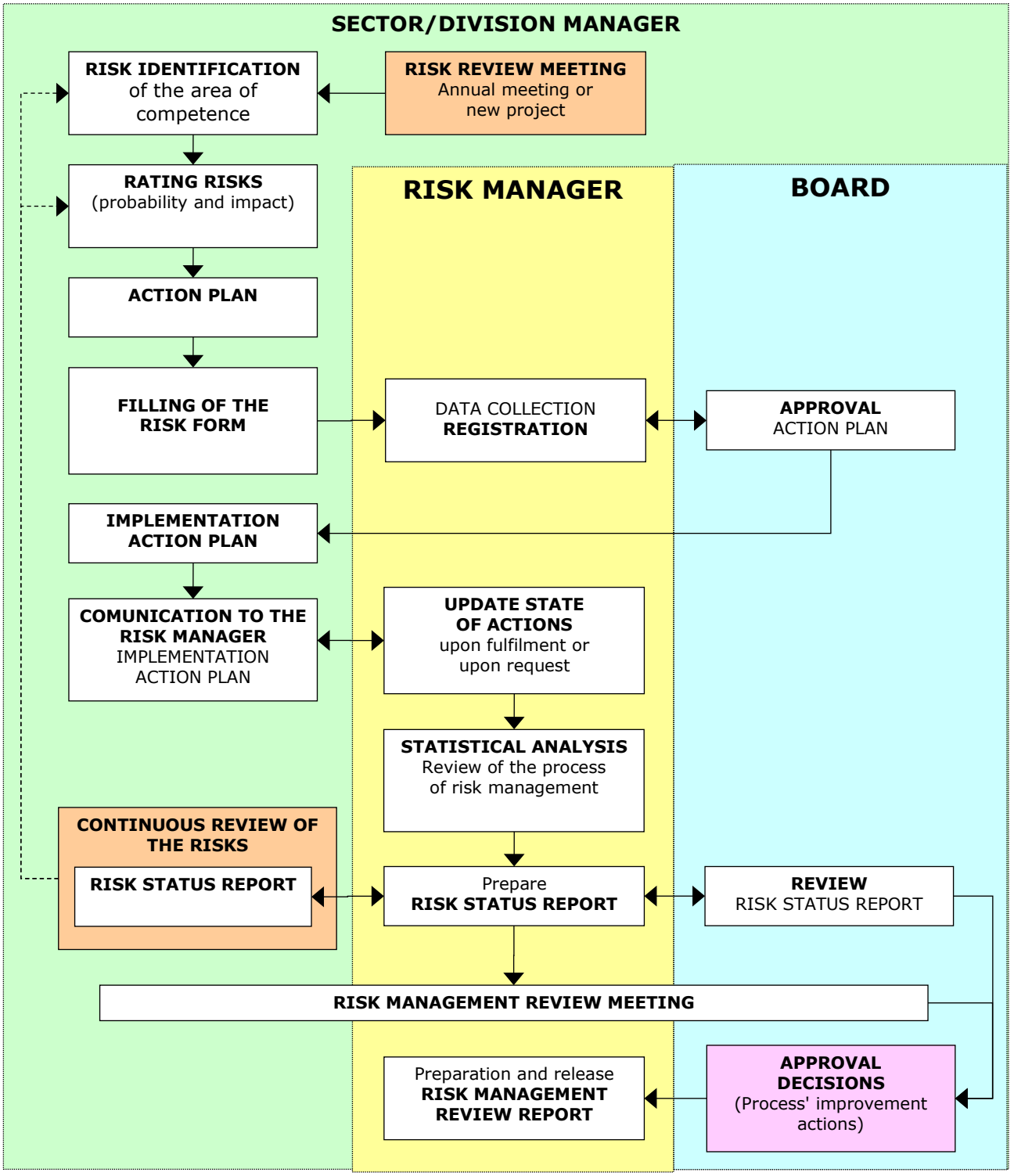
C (criticality coefficient) = P * I

		IMPACT			
		1	2	3	4
PROBABILITY	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4

The laboratory management shall assess the risk level and take decisions if the risk is acceptable without any further action.

The lowest risk, green in color, might be classified as an acceptable risk, while the highest risk, red in color, may requires immediate action. Yellow will have intermediate ratings. Risks having low rating due to a low likeliness but with high impact may require additional consideration.

WHO DOES WHAT?



RISK CATEGORIES

E	C	RISK	DESCRIPTION
FINANCIAL			Risks associated to continued business brought about by the lack of financial stability which includes funding position, bank credit, debit collection possibilities and trading performance as well as ability to maintain competitive product prices.
P	I	**BUDGET**	Availability or allocation of resources.
P	I	**CAPITAL INVESTMENT**	The making of appropriate investment decisions.
P	I	**FRAUD OR THEFT**	Unproductive loss of resources.
STRATEGIC			Risks associated with maintaining Customer commitments and market domination through the supply chain, supply sourcing policies, openness with programs and their problems, responsiveness to customer changing needs, total manufacturing capacity and technologies (plus potential for development), type/number of customers, joint-ventures, revenue sharing, etc. Willingness and ability to implement and maintain security and confidentiality polices shall also be considered.
B	E	**MARKET**	Competitors and market investigation.
B	I	**COMMERCIAL**	Marketing and communications, commercial policies, exploitation of opportunities to make gains.
B	I	**INFRASTRUCTURE**	Transport systems, power supply systems, suppliers, business relationships with partners, dependency on internet and e-mail, etc.
B	E	**TECNOLOGIC**	Use of technology to achieve objectives.
POLITICAL / ECONOMIC			Risks resulting from National/International trading that could be affected by differing Government polices and effects of Government ownership and subsidization, cultural, language and employment legislation, etc.
B	E	**ECONOMIC**	Economic factors such as interest rates, exchange rates, inflation.
B	E	**IMPORT/EXPORT**	Import and export controls and duties.
ETICS / LEGAL			Risks associated with the non application of fair/appropriate business practices, fraud, non compliance to Equal Employment Opportunity requirements and Child Labor Acts, responsibilities to customers/stakeholders/users, suppliers/sub-tires and employees. This includes risks on how the company is perceived by the customer, employees and general public.
B	E	**LAWS AND REGULATIONS**	Laws and regulations which if complied with should reduce hazards.
B	I	**IMMAGINE**	Public reputation of the organisation and consequent effects.
ENVIRONMENT AND PEOPLE			Risks associated with product development, manufacturing, materials and support that can adversely have an impact on the environment and people.
P	I	**ENVIRONMENT**	Fuel consumption, pollution, etc.
P	I	**HEALTH AND SAFETY**	Relating to the wellbeing of people, work environment.
HUMAN FACTOR			Risks associated with Staff turnover, available skills and training, employment levels, staff relationships and management expertise; employer to employee relationships and willingness, and ability to communicate effectively with suppliers and customers. They include human needs, expectations, attitude, motivation as well as anthropometric factors (physical dimensions of the human being).

E	C	RISK	DESCRIPTION
P	I	**PERSONNEL**	Availability and retention of suitable staff.
TECHNICAL / MANAGEMENT			Risks associated with the ability to deliver on time, to quality and cost as well as the ability to develop market share, improve lead times, prices, quality, etc. and improve/maintain customer support. Ability to respond to program changes and customer needs (modifications, build schedules, delivery etc.).
P	I	**PROJECT**	Project planning and management procedure.
P	I	**TIMING**	Deadlines, time schedule.
P	I	**CUSTOMERS**	Customer needs and requirements.
T	I	**SPECIFICATIONS AND REQUIREMENTS**	Requirements clear specification and verification, system specifications.
T	I	**TECHNICAL**	Design complexity, control of interfaces, tooling, new technology, etc.
PLANNING			Including Physical/Environmental Risks to the Supply Chain as a consequence of potential disaster based on geographic location such as potential flood, earthquake, extreme changes to climatic conditions, production techniques/materials or the effects of production bottlenecks, logistics, facilities, resources, prima material availability, fire/explosion, insurrection etc. are all to be considered in terms of protection and contingency planning for the Supply Chain. Risk issues associated with production/logistic planning of the material to be furnished, including sub-tier supplier planning activities shall also be considered.
P	E	**NATURAL DISASTERS**	Fire, flood, earthquake.
P	I	**LOGISTIC**	Production/logistic planning of the material to be furnished, including sub-tier supplier planning activities.

RISK REGISTRATION FORM

FORM NUMBER	Alphanumeric code (assigned to the card by the risk manager) as follows: RF 000 where “000” is the progressive number of unique identification of the form.
HEADING FORM	Specify the business function issuing the form, the date the form was issued, and the business site or sites to which the risk applies.
FORM APPROVAL	Signature of approval of the Chairman of the Board of Directors or his delegate.
EVENT	Describe the event that may cause the risk
KIND OF RISK	Specify the type of risk reported, in accordance with procedures or other reference documents.
PROCESS STEP	Specify the process phase on which the reported risk impacts, in accordance with procedures or other reference documents.
RISK DESCRIPTION	Describe in detail the risk highlighted, specifying both the cause and the effect on the program / project of applicability.
INITIAL PROBABILITY (P_A)	Evaluate the probability that the risk will occur, in the situation and with the conditions existing at the date of issue of the form, assigning a score from 1 to 5 increasing with the degree of probability.
INITIAL IMPACT (I_A)	Evaluate the impact that the risk could potentially have on the program or project of applicability, in terms of costs, planning and / or performance, in the situation and with the conditions existing at the date of issue of the form, assigning a score from 1 to 5 increasing with the degree of impact.
INITIAL CRITICALITY (C_A)	Initial risk criticality indicator, reference for defining the degree of risk priority and consequently the urgency of recovery actions. It is obtained by multiplying the impact and probability factors described above.
CHECKS ALREADY EXISTING	Describe any procedures and actions already in place within the company, at the date of issue of the form, useful / usable for risk control purposes, which may be integrated and / or revised and improved in the action plan proposed in the form.
RISK MITIGATION ACTION	Brief description of the program of activities necessary for the elimination of the risk or for its reduction to an acceptable level. Based on the number of actions required and the complexity of the program (costs, personnel involved, duration, etc.) the action plan can be issued as a separate document. In this case, only the document reference number will be shown on the form.
RESIDUAL PROBABILITY (P_A)	Evaluate the probability that the risk will occur again, after the implementation of the action plan, assigning a score from 1 to 5 increasing with the degree of probability.
RESIDUAL IMPACT (I_A)	Evaluate the impact that the risk could potentially still have on the applicability program or project, in terms of costs, planning and / or performance, after the implementation of the action plan, assigning a score from 1 to 5 increasing with the degree of impact.
RESIDUAL CRITICALITY (C_A)	Residual risk criticality indicator, reference for defining the estimated effectiveness of the action plan. It is obtained by multiplying the impact and probability factors described above.
IMPLEMENTATION DATE	Specify the estimated times for the implementation of the plan and risk reduction / elimination.
REVISION DATE	Specify the date on which the risk will be reviewed considering the evolution of the scenario.
RISK MANAGER	Person of the company responsible for the development and management of the risk recovery action plan (function manager or his / her delegate).