INTERNATIONAL WORKSHOP AGREEMENT

IWA 31

First edition
2020-03

Risk management — Guidelines on using ISO 31000 in management systems

Reference number
IWA 31:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

International Workshop Agreement IWA 31 was approved at a workshop hosted by BSI, held virtually by Zoom in December 2019.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

There is a steady growth in the number of organizations, of all types and sizes, that are using management systems based on an ISO and IEC Management System Standard (MSS)[1)]. New ISO and IEC MSS continue to be developed to address specific aspects of an organization's activities, products or services. The ISO/IEC Directives, Part 1 specifies the high level structure (HLS) for MSS. This generic structure prescribes identical core text, common terms and core definitions for all ISO and IEC MSS. An organization can integrate requirements or recommendations of different MSS into their management system. The unified structure of MSS can make it easier for users to construct an integrated management system (IMS), rather than end up with a fragmented management system. All such MSS employ the concept of an approach based on risk management, a risk-based approach or risk-based thinking (depending on the terminology used within the management system in question), which is at the core of any management system. The main advantage of this is the holistic application of interrelated systems. ISO 31000:2018 can be used to further develop or improve an IMS through its guidance on how to determine the risks that need to be addressed to give assurance that the management system can achieve its intended outcomes, enhance desirable effects, prevent or reduce undesired effects, and achieve continual improvement.

ISO 31000 is international best practice regarding risk management, which is widely accepted, generic and open to manage any type of risk. Integrating risk management into its management system(s) by using ISO 31000 brings multiple benefits to an organization, whether they only address negative effects or include positive effects. The purpose of risk management as outlined in ISO 31000 is the creation and protection of value. It helps improve the decisions of risk owners or process owners and enhances the operations of processes and all other activities of the organization, including strategic and operational. This can lead to better results, higher output quality, less costly mistakes and the management of liability.

Integrating risk management in accordance with ISO 31000 creates and protects value in organizations by supporting the achievement of objectives and making the organization more resilient to adverse effects. Assessing risks enables their appropriate treatment and establishes a basis for increasing the effectiveness of the organization's management system, achieving improved results, and preventing negative outcomes. However, integrating risk management into a management system can pose challenges, which can be reduced by following the guidance in this document.

1) A list of ISO and IEC MSS is available at: https://www.iso.org/management-system-standards-list.html

Risk management — Guidelines on using ISO 31000 in management systems

1 Scope

This document gives guidelines for integrating and using ISO 31000 in organizations that have implemented one or more ISO and IEC Management System Standards (MSS), or that have decided to undertake a project implementing one or more MSS incorporating ISO 31000. This document explains how the clauses of ISO 31000 relate to the high level structure (HLS) for MSS.

This document does not provide guidance on implementing a management system in general. It does not specify requirements of a MSS. It does not provide a summary of ISO 31000; however, it does, as explained above, provide the background for understanding ISO 31000. Using this document does not remove the need to use other standards to address specific aspects of risk.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 31000:2018, *Risk management — Guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 31000:2018 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

4 The use of the term “risk” in ISO 31000 and other standards

The application of terminology should be taken in the context within which it is applied. For an organization’s risk management, ISO 31000:2018, 3.1, defines “risk” as the “effect of uncertainty on objectives”. Some standards do not refer to objectives, but the text regularly states that risks need to be addressed in order to give assurance that the management system can achieve its intended outcomes. An objective can be expressed as an intended outcome or result.

The risk management framework and process of ISO 31000 are customized and proportionate to the organization’s external and internal context related to its objectives. This includes the interested parties’ perspectives.

There are some contexts where different terminology is used (e.g. safety, occupational health and safety, medical devices sector). This use implements a general understanding of the term “risk” that narrows the ISO 31000 concept of risk in that it focuses on the potential negative impact of deviations from the expected. This approach can be considered to be included in the broader definition of risk in ISO 31000:2018, 3.1.

5 Guidance on ISO 31000 for users of MSS

ISO 31000:2018 offers guidance to all types of organizations, regardless of type and size, and is written for people who create and protect value in organizations by managing risks, making decisions, setting purpose and strategy, achieving objectives, and improving performance.

The eight principles of risk management act as a foundation for the creation and protection of value. These provide guidance on the characteristics of effective and efficient risk management, communicating its value, and explaining its intention and purpose. ISO 31000 provides a common approach to managing any type of risk faced by an organization throughout its life.

The purpose of the risk management framework is to assist the organization in integrating risk management into significant activities and functions. The effectiveness of risk management will depend on its integration into the governance of the organization, including decision-making.

The risk management process as set out in ISO 31000 should be customized proportionate to the external and internal context of the organization related to its objectives. It should be adapted so that it becomes an integral part of the management system, and is integrated into the structure, operations and processes of the organization.

Using the guidance on principles and framework, an organization may choose to customize the application of the risk management processes to its management system for any type of risk it faces throughout its life. Adding the steps of the risk management process can enhance the management system. In this context, it needs to be remembered that although the risk management process is often presented as sequential, in practice it is iterative.

Risk management should be applied whenever there is any information or estimation that initiates or adds to a process or activity, or whenever there is a change in the context of the organization.

There could be a degree of uncertainty in this information or estimation, which could have an effect on the achievement of objectives. An effect is explained in ISO 31000:2018, 3.1, as a deviation from the expected, which can be positive, negative or both. Therefore, the organization should revisit risk identification whenever there is new information or estimations relevant for its process and activities.

Figure 1 shows an overlay of the ISO 31000 guidelines with the framework of the generic HLS clauses for MSS. The top row references the HLS clauses and the left-hand column represents the ISO 31000 framework clauses. For example, looking at the intersection of ISO 31000:2018, 5.2, on leadership and the HLS clause on leadership, the grey key indicates there should be a process referring to the management of risk. Therefore, this table can be used as a reference point. For details on the clause connections, see Table A.1.

ISO MSS HLS clauses →	Context	Leadership	Planning	Support	Operation	Performance	Improvement
ISO 31000 guidelines and framework ↓	ISO 31000:2018, 5.1: "The purpose of the risk management framework is to assist the organization in ***integrating*** risk management into significant activities and functions."						
4. Principles							
5.1 General							
5.2 Leadership							
5.3 Integration							
5.4 Design							
5.5 Implementation							
5.6 Evaluation							
5.7 Improvement							
6.1 General							
6.2 Communication							
6.3 Scope, context							
6.4 Risk assessment							
6.5 Risk treatment							
6.6 Monitor, review							
6.7 Record, report							

Figure 1 — Relationship between ISO 31000 and the clauses of the HLS for MSS

6 Integrated management systems and using ISO 31000

The application of risk management can be done through the process approach of a management system. The ISO 31000 framework should be merged with the management system by applying a gap analysis to include ISO 31000 framework components. By integrating risk management into the process approach, duplications or conflicts are avoided.

In order to achieve effective and efficient integration and implementation of the ISO 31000 framework and its process into other MSS, the organization should adopt ISO 31000 principles. The ISO Handbook *The Integrated Use of Management Systems Standards (IUMSS)*[5] could be a useful reference in this respect. For detailed steps for integrating the use of MSS, it is advised to refer to this handbook.

Annex A provides guidance on how on organization can approach the integration of management of risk into its MSS. Annex B is a case study of incorporating ISO 31000 into a multidiscipline management system.

Annex A
(informative)

Correspondence between ISO 31000 and the HLS for MSS

Table A.1 shows the linkages between the main clauses of ISO 31000 and the most important correlating clauses of the HLS for MSS. Users of ISO 31000 can integrate risk management practices into the management system of the organization where these clauses of the HLS are addressed.

Table A.1 — Correspondence between ISO 31000 and the HLS for MSS

Clauses of the HLS for MSS		Clauses of ISO 31000:2018		
		4. Principles[a]	5. Framework	6. Process
4. Context of the organization	4.1 Understanding the organization and its context	0, a), c), e), f), g)	5.2, 5.4.1	6.1, 6.3.1, 6.3.3, 6.3.4, 6.6, 6.7
	4.2 Understanding the needs and expectations of interested parties	0, a), c), d), e), f), g)	5.2, 5.4.1, 5.4.5	6.1, 6.2, 6.3.1, 6.3.3, 6.3.4, 6.6, 6.7
	4.3 Determining the scope of the XXX management system	0, a), c), f)	5.1, 5.2, 5.4.1, 5.5	6.3.1, 6.3.3, 6.3.4
	4.4 XXX management system	0, a), b), c), f)	5.1, 5.2, 5.3, 5.4.1, 5.5	6.3.1, 6.3.3, 6.3.4
5. Leadership	5.1 Leadership and commitment	0, a), c), d), g)	5.1, 5.2, 5.4.2, 5.4.4	6.2, 6.6, 6.7
	5.2 Policy	0, a), c), d), g)	5.2, 5.4.2	6.2, 6.6, 6.7
	5.3 Organizational roles, responsibilities and authorities	a), c), d), g)	5.2, 5.4.3	—
6. Planning	6.1 Actions to address risks and opportunities	0, a), b), e), f)	5.1, 5.4.2, 5.7.1	6.1, 6.4, 6.5
	6.2 XXX objectives and planning to achieve them	0, a), b)	5.4.2, 5.7.2	6.5
7. Support	7.1 Resources	0, a), f), g)	5.1, 5.4.4	6.3.4, 6.5.2
	7.2 Competence	0, a), f), g)	5.1	—
	7.3 Awareness	0, a), f), g)	5.1	—
	7.4 Communication	0, a), d), f)	5.1, 5.4.5	6.1, 6.2, 6.3.4
	7.5 Documented information	0, a), f)	5.1	6.1, 6.7
8. Operation	8.1 Operational planning and control	0, a), b), f)	5.1, 5.3, 5.5, 5.7	6.1, 6.4, 6.5, 6.6, 6.7
9. Performance evaluation	9.1 Monitoring, measurement, analysis and evaluation	a)	5.6	6.1, 6.3.3, 6.3.4, 6.4.1, 6.6, 6.7
	9.2 Internal audit	a)	5.6	6.1, 6.3, 6.4.1, 6.6, 6.7
	9.3 Management review	0, a), b), e), g)	5.6, 5.7	6.1, 6.3, 6.4.1, 6.6, 6.7
10. Improvement	10.1 Nonconformity and corrective action	0, a), h)	5.7	6.1, 6,4, 6.5, 6.6
	10.2 Continual improvement	0, a), h)	5.1, 5.2, 5.7	6.1, 6.4, 6.5, 6.6

[a] Principle "0" refers to the core principle "value creation and protection".

NOTE The subclause numbers in the cells refer to the subclauses of ISO 31000:2018 according to relevant column heading.

Annex B
(informative)

Case study incorporating ISO 31000 into a multidiscipline management system

B.1 General

This case study illustrates a holistic approach for risk management in an organization, across multiple disciplines, based on the principles of ISO 31000 and the HLS for MSS. This case study does not provide any guidance on how to approach the integration of ISO 31000 into an organization's management system(s). It also does not include requirements related to each of the referenced MSS.

For the purpose of this annex, only the aspects of some clauses/requirements (those considered particularly effective) are highlighted to show how the application of requirements to the quality management system (QMS) processes of the organization were reviewed in the light of a risk management approach.

The text used in the case study represents the following:

— *italic text*: provides the perspective of the organization;

— regular text: provides guidance.

NOTE In this annex the term "interested party" has been used because it is the term used by this organization, which has applied ISO 9001 since 1997. According to the definition of "stakeholder" in ISO 31000:2018, 3.3, the term "interested party" can be used as an alternative.

B.2 Description and background of the organization

"XYZ" is a fictional organization used for the purpose of this annex.

— It comprises about 120 people.

— It concerns the development, trading, technical assistance and production, by mixing powders and liquids, of:

  — chemical products for material surface treatment;

  — chemical products for waters treatment;

  — lubricants for mechanical processing;

  — chemical auxiliaries;

  — temporary protective films and adhesive systems for the aerospace industry.

— It is a for-profit corporation.

— It needs to consider the regulatory environment, e.g. for the EU, Canada and Colombia, in regard to topics such as disposal requirements, chemical waste requirements, transportation requirements, safety requirements, etc.

— It has a distributed geography with two plants (Canada-Toronto and Colombia-Bogota) and one head office based in Brussels.

The organization has been ISO 9001 certified since 1998.

Since the certification to ISO 9001, there have been additional requirements from customers to work with other MSS to manage environmental and health and safety aspects, which were used as separate systems.

By the end of December 2017, the quality manager (QM) became aware of the possibility for integrating risk management in accordance with ISO 31000 in the company management system starting from the well-consolidated QMS.

After discussing the study and its advantages with the CEO and having had their approval in principle, the QM suggested to the CEO to attend a seminar together in which organizations from three different sectors will share their own experience on the use of ISO 31000, including the transition from the 2009 to the 2018 edition. By the end of the seminar, the CEO and QM realized the value of implementing a risk management framework to support their management systems and made the decision to move forward.

The risk management approach should be integrated into the existing ISO 9001 management system. The CEO and Board of Directors assigned the responsibility and the authority to the QM for arranging a detailed project stating intentions and directions of the risk management approach, in accordance with ISO 31000. They also instructed all the process owners with the task of actively cooperating with the QM in both preparing and implementing the project.

Those intentions and directions were then incorporated into the integrated policy. Some examples are given below:

— *risk is an integral and unavoidable component of our business, every activity that helps the organization to pursue objectives introduces new risks to the organization;*

— *we are committed to managing all risk in a proactive and effective manner;*

— *risk assessment will be applied to all aspects of our business by the management, governing body and operations at appropriate levels;*

— *we promote a risk-aware culture in all decision-making, so we foster the spread of risk-based thinking, aimed at taking advantage of opportunities and preventing undesirable results;*

— *risk-based thinking refers to this risk-aware culture that must be well-established at all levels in our organization as an essential part of the "organizational knowledge";*

— *everyone in our organization has responsibility for managing risk, within their respective areas of competence and the limits of the assigned authority, responsibility and accountability;*

— *clients are increasingly expecting the organization to act ethically, and this applies to all aspects of our processes, that directly or indirectly contribute to value;*

— *commitment to risk management extends to all of our suppliers;*

— *our risk criteria (both to evaluate the significance of risk and to choose among the treatment options) are based on our code of ethics and particularly on the right balance of the three pillars of sustainability (environment, social, economic): cost and benefit are to be both evaluated in terms of sustainability;*

— *we will also apply risk management in order to control any kind of legal risks, helping us to fulfil all our compliance obligations.*

B.3 Application of risk management (from ISO 31000) in the existing QMS

The QM realized that all clauses should have been involved to some extent in the project for the application of risk management in the existing QMS (hereinafter referred to as the "project").

First, the project was based on the consideration that the components of the risk management framework should be embedded within the organization's overall strategic and operational policies and practices. This means that the first step was a review of each element of the QMS in order to identify and evaluate any gaps

of the existing risk management practices. The second step was the filling of those gaps by integrating the components of the risk management framework into the interrelated and interacting elements of the QMS (i.e. the organization's structure, roles and responsibilities, planning and processes to achieve its objectives).

Apart from the clauses of ISO 9001:2015 where risk (associated to opportunity and threat) is explicitly mentioned, there are direct or indirect implicit references to risk and risk management in almost all of the clauses and relevant requirements.

The considerations below were taken into account by the organization.

Planning *(Clause 6) was considered a key clause for risk management, because it is inherent within the concept of influence of uncertainty in relation to objectives.*

Understanding the organization and its context *(4.1) was the basis for both establishing the processes of the management system and framework and process of risk management. The determination of the relevant interested parties and their needs and expectations was the basis for establishing the management system and its processes as well as establishing the risk criteria. The requirements related to communication (see ISO 9001:2015, 7.4) had been supplemented with suggestions about communication and consultation in ISO 31000:2018.*

Documented information *(7.5): ISO 9001 (as per the HLS) requires, in addition to the documents expressly referred to in the standard, all documented information determined by the organization as being necessary for the effectiveness of the QMS. The project stated that risk management had to be used to determine which documents, in addition to those required by the standard, were necessary and what their degree of detail should have been. In addition to considering the size of the organization, the type of activity, the complexity of the processes, their interactions and the competence of the personnel, the questions to be asked might have been basically two, for each process:*

a) *What negative impacts could the lack of documented information (procedures, instructions, records or a low degree of detail) generate?*

b) *What positive impacts could be generated by entering a new procedure, an instruction, a registration or improving the level of detail of existing ones?*

It was kept in mind that documents that are too large or more detailed than necessary run the risk of being completely ignored.

There was a determination of the ***processes*** *(4.4) required for the management system and their application throughout the organization, regardless of whether these processes are performed internally or outsourced. For each process (internal or external) with a significant uncertainty, the project stated that it was necessary to identify:*

— *activities that transform inputs into outputs;*

— *results to be achieved;*

— *potential effects, positive or negative, on downstream processes and on the final product;*

— *the controls, the monitoring, the measurements that should have been such as to be able to maximize positive impacts (seizing opportunities for improvement) and minimizing negative ones (avoiding unwanted events, nonconformities).*

Documented information such as procedures, work instructions, specifications, etc. contained actions to address risks in order to ensure that the QMS processes can achieve their intended results, enhance desirable effects, prevent or reduce undesired effects, and achieve improvement.

There is a close relationship between risk management and decision-making that is clearly stated and confirmed in many clauses throughout ISO 31000:2018. Therefore, the application of risk management enables, among other things, the fulfilling of one of the quality management principles: evidence-based decision-making.

*Also, the first part of **Support** (7.1, 7.2 and 7.3), although it does not contain explicit references to risk management, was interpreted in this light in order to provide resources (personnel, infrastructures and work environment) such as to make it possible to seize opportunities and avoid unwanted events, pursuing the main objective of satisfying more and more customers, as well as other relevant interested parties. The personnel must have the necessary competence and resources to keep the risks related to their activity under control. All persons were made aware of all the kinds of risks they face and of their contribution to the achievement of organization's objectives.*

*The choice of **monitoring and measuring resources** (ISO 9001:2015, 7.1.5, and 9.1), their metrological characteristics and the calibration intervals, etc. was established, taking into account all related risks, results of previous monitoring and measurement activities, and taking into account not only threats and dangers, but also opportunities to be seized. This concerns the importance of having or not having certain measurements, the tolerances required, the acceptable measurement uncertainty, the possibility of an instrument drift between one calibration and another, and the degree of detail for records. All aspects were decided in the light of a risk assessment and a cost-benefit analysis.*

***Operation** (Clause 8) is a key clause and risk management was strictly applied to the implementation of all its requirements in ISO 9001. The determination of requirements for products and services, the relationship with customers, and the design and development of products and services were all affected by the consideration of related opportunities and threats.*

*Risks related to the **supply chain** are a particularly critical aspect in companies where outsourcing is frequent. Risk management was considered a key activity regarding the control of externally provided processes, products and services. The type and extent of control applied to the external provider and to the externally provided processes, products and services must depend on the effect on the subsequent production and service provision.*

*In order to establish the controlled conditions for **production and service provision**, as well as all the related aspects (e.g. think about identification and traceability, preservation or control of changes), the application of the risk management process assumed a great importance.*

***Performance evaluation and improvement** was addressed keeping in mind the "monitoring and review" activities suggested in ISO 31000:2018, 6.6, as well as the aspect of the framework about evaluation and improvement (5.6 and 5.7).*

***Recording and reporting** (see ISO 31000:2018, 6.7) was implemented to the extent required by the actual need to record and document the risk management in relation to the significance of the risks.*

The project also considered the following.

***Quality-related risks** can affect objectives in the following areas (non-exhaustive examples):*

— *compliance obligations of products, services and operation;*

— *competition and competitors;*

— *the success of products and services, customers and other interested parties' satisfaction;*

— *the sustainability of products, services and processes;*

— *the organization's sustained success, image and reputation.*

In relation to above objectives, quality-related risks can be affected by uncertainties, which can arise, as example, from:

— product innovation and technological changes;

— changes in the supply chain;

— compliance obligations;

— views of the interested parties in relation to ethics, principles, values and expectations;

— information security;

— the reliability of infrastructure.

B.4 Integration of other MSS

The implementation of the ISO 31000 principles, framework and process highlighted that the silo approach should be abandoned in favour of a wider, integrated and coherent management of the organization and relevant risks. The CEO and Board of Directors realized that it was time to follow the philosophy of enterprise risk management (ERM), which takes into consideration all kind of risks and manages them in an integrated and coordinated way.

Very often risks involve more than a single discipline in a transversal way. In some special cases, an opportunity in one discipline (e.g. for quality) could pose a threat for another one [e.g. for environment or occupational health and safety (OH&S)] and vice-versa. This is another reason why it is better to manage disciplines and relevant risks in an integrated and coordinated way with the support of the necessary competence in different disciplines.

This integrated approach also reminded the organization that risk treatment can create new risks or modify existing ones.

It means a strict approach to the assessment of risk, to any kind of risk of whatever nature, which affects strategic and operational objectives. It enables the organization to identify and address not only threats, but also those opportunities that can be exploited in order to gain a competitive advantage. This is also the philosophy of the HLS for MSS.

Furthermore, all elements considered in order to integrate a risk management framework into a QMS (see above) are almost all useful and valid for risk management in the field of other disciplines such as the environment and OH&S, as well as information security.

Moreover, some MSS, e.g. ISO 14001, ISO/IEC 27001 and ISO 45001, have requirements for risk assessment and risk treatment. Organizations predominantly focus on controlling potential threats and could overlook opportunities that the situation could present.

All these considerations led to the decision of:

a) *creating a single "integrated management system" covering in a harmonious and coordinated way the three disciplines: quality, environment, and health and safety (QEH&S);*

b) *achieving certification of ISO 45001 by the first half of 2019;*

c) *assigning to the QM the responsibility and authority for coordinating the establishment, implementation, maintenance and continual improvement of the IMS, with the embedded risk management framework and process; the QM is also the person in charge of supporting the whole organization with reference to risk management;*

d) *all process owners in the organization are also risk owners, i.e. have the accountability and authority to manage risk within their area of responsibility, and they also provide the discipline-specific knowledge and skills in support of the QM.*

The organization also considered the following generally accepted concepts.

— Environment-related risks and OH&S-related risks are those risks that are affected by, or concern, issues relevant to the environment and to OH&S, respectively.

— Environment-related risks are mainly risks to the environment arising from the possibility that an environmental aspect causes environmental impacts.

— OH&S-related risks are mainly risks to the health and safety of workers arising from the possibility that a work-related hazardous event or exposure causes harm (injury or damage to the health of people).

— Uncertainty generally comes into play in terms of operational control and mechanisms designed to manage environmental aspects and health and safety aspects. There is some chance that the controls/mechanisms will fail or not be effective, which could result in an adverse impact/undesired effect.

— Both environment-related and OH&S-related risks are also a category of risks to the organization arising from the uncertainty that environment-related or OH&S-related issues or matters can cause one or more consequences, whether adverse or beneficial. These risks can concern (but not limited to):

  — compliance obligations, product liabilities, the cost of litigation and injury-related costs;

  — the well-being, performance or productivity of workers;

  — permission for development and operational activities;

  — the organization's image and reputation, and confidence in the organization's business;

  — competition and competitors;

  — weather variability and climate change;

  — damages from natural events, which can also include adverse environmental impacts;

  — business continuity.

B.5 Integration of information security MSS (ISO/IEC 27001)

The organization had not been insensitive to the challenges posed by globalization and digital transformation that drive enterprises to exploit business opportunities offered by new markets and new ICT. It was aware that changes connected to the exploitation of new opportunities can pose other threats and other opportunities for almost all disciplines addressed within a management system. The awareness that information-security-related risks affect the organizational context was the reason behind the search for opportunities in order to improve information security.

The structured and systematic application of risk management process led the organization to apply Industry 4.0 and Internet of Things (IoT) and the plan for digital innovation.

Examples of considerations in this context include the implementation, replacement or reconfiguration of sensors and techniques (big data analytics, artificial intelligence, as well as the cloud and GPS, where applicable) for the monitoring and control of:

— production processes, with the aim of improving efficiency, balancing flows of materials and semi-finished products, and effectiveness (defectiveness of the final product);

— the life cycle of the product, with the aim of improving the management of the supply chain (including its risk management);

— production infrastructures, with the aim of enabling the predictive maintenance processes in partial or total replacement of traditional maintenance processes (reactive maintenance can be costly and dangerous);

— OH&S devices and infrastructures and PPE (wearable) in order to carry out a real-time monitoring and control, with the aim of improving working conditions and individual well-being;

— environmental aspects.

Considering the introduction of new ICT has given rise to the need to manage the new technology-related risks. A decision was made to also implement ISO/IEC 27001. The organization's top management was guided by the following statements:

— *in the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives;*

— *information security risks are associated with the potential that threats will exploit vulnerabilities and thereby cause harm to the organization;*

— *information security objectives relate to the primary impacts of innovation in the following areas:*

  — *the effectiveness of the governance of the organization as it is based on the DIKW pyramid (i.e. Data, Information, Knowledge, Wisdom together with applications, services and systems to handle them);*

  — *assurance that its information is adequately protected against threats (malfunction and or cyber attack) on a continual basis;*

  — *image and reputation related to organization's ability to protect personal data, customers' data and know-how, as well as its own data;*

  — *the preservation of information quality related to the following information security requirements:*

    — *confidentiality (property that information is not made available or disclosed to unauthorized individuals, entities or processes);*

    — *integrity (property that information is accurate and complete);*

    — *availability (property of being accessible and usable on demand by an authorized entity) of information;*

  — *business continuity.*

There are also some important and indirect impacts of information security on the objectives of other "disciplines" within the organization's operations.

When the organization decided to pursue the opportunity offered by new ICT-related technologies, the potential expected benefits were in the fields of:

— *environment protection;*

— *preventing work-related injury and ill-health;*

— *improving productivity and the quality of products and services offered;*

— *enhancing the organization's performance in terms of the triple bottom lines (people, planet and profit).*

All the opportunities offered by new ICT pose some significant threats which, together with hardware and software vulnerabilities, have the potential to give rise to new ICT-related risks. That is why the organization should identify the need to establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of ISO/IEC 27001.

B.6 Conclusion

The application of risk management in management systems, which is based on requirements in one or more MSS, in accordance with the guidance provided in ISO 31000, should be a central focus of an organization.

The implementation of this project has proved to be a winning choice.

It has been carried out with a view to integrate concepts from different sectors into one management system. It constitutes an example of the adoption of a holistic approach, taking advantage of the synergies provided by the integration of guidelines in ISO 31000 and requirements in some MSS (such as ISO 9001, ISO 14001, ISO/IEC 27001 and ISO 45001).

A systematic, comprehensive and relevant approach should be taken to manage all risks, associated to opportunities and threats, as it helps the organization to achieve its strategic business objectives, while creating and protecting value for all its relevant interested parties.