Received: 21 May 2018 | Revised: 6 July 2018 | Accepted: 12 July 2018
DOI: 10.1002/smr.1984

SPECIAL ISSUE PAPER

WILEY Journal of Software: Evolution and Process

ISO 31000-based integrated risk management process assessment model for IT organizations

Béatrix Barafort[1] | Antoni-Lluís Mesquida[2] | Antònia Mas[2]

[1] Luxembourg Institute of Science and Technology, 5 Avenue des Hauts-Fourneaux, L-4362 Esch-sur-Alzette, Luxembourg

[2] Department of Mathematics and Computer Science, University of the Balearic Islands, Cra. De Valldemossa, km 7.5, Palma de Mallorca, Spain

Correspondence
Antoni-Lluís Mesquida, University of the Balearic Islands, Department of Mathematics and Computer Science, Cra. De Valldemossa, km 7.5, Palma de Mallorca, Spain.
Email: antoni.mesquida@uib.es

Funding information
Spanish Ministry of Science and Technology, Grant/Award Number: TIN2016-76956-C3-3-R

Abstract

Governance, Risk management, and Compliance activities are key challenges faced by organizations. Process Models and Capability Process Assessments are governance instruments that can help organization in assessing and improving their processes. Several ISO standards propose process models for Management System Standards based on ISO 9001, ISO/IEC 20000-1, and ISO/IEC 27001, and for project management with ISO 21500. The ISO 31000 standard provides guidance for Risk management with a process approach and systemic perspective. This paper presents an ISO 31000-based Integrated Risk Management Process Assessment Model (PAM) for IT organizations enabling to integrate on an easy way several ISO process-oriented standards which are often targeted by IT organizations. This PAM integrates risk management dimensions with ISO 9001, ISO 21500, ISO/IEC 20000-1, and ISO/IEC 27001. It offers a centralized and integrated risk management approach which provides the basis to improve, coordinate, and interoperate risk management activities.

KEYWORDS

integrated risk management, ISO, ISO 31000, IT organizations, process assessment model, process assessment model engineering, transformation process

1 | INTRODUCTION

Governance, Risk management, and Compliance activities are key challenges in organizations. With the era of digitalisation, the governance of digital transformations is a critical topic, with many instruments and ways of maintaining operations with an adequate organization and in a growing regulation landscape. Risk management is part of these key challenges and is related to a multitude of domains, for IT and non-IT concerns. Process performance is one of many ways of governance, with process improvement to enhance practices. To rely on processes is essential for companies. Capability and Maturity Models (C&MM) support process improvement with process assessment facilities. They provide a guide and a structure for a process improvement roadmap. There are plethora of process models for various business domains and sectors. At the International Standardization Organization (ISO), there are several published Process Reference Models (PRM) and Process Assessment Models (PAM) in different kinds of domains[1-4]; these various initiatives are based on the ISO Process assessment standard series concepts[5]; they rely on a very structured and systematic approach for process assessment and guided process improvement.

Our research works[6] have already investigated risk management activities in IT organizations (IT organizations meaning any IT department or IT company needing to integrate risk management activities) by comparing how risk is tackled in various ISO standards targeting management systems (also named Management System Standards or MSSs) for: quality perspectives in ISO 9001,[7] information security management in ISO/IEC 27001,[8] IT Service management (ITSM) in ISO/IEC 20000-1,[9] and project management in ISO 21500[10] (these IT-related and non-IT standards have been selected by the authors because they are significant for many companies and were reported back to the authors by practitioners; ISO 9001, ISO/IEC 20000-1, and ISO/IEC 27001 are very popular management systems, documented as integration vectors in literature as mentioned in Barafort et al[6]). This comparison had shown how to pave the way for a centralized and integrated risk management. That provides the basis to improve, coordinate, and interoperate risk management activities in IT organizations. This integration is particularly enforced by ISO standards which propose approaches that are the results of international consensus and that are often requested by the market (ie, ISO 27001 certification). It is especially true for the ISO 31000[11] standard (in its latest published version) for Risk management, which is our Ariadne's thread. In addition, with the study of the various topics such as quality management, information security management, ITSM, and project management, we can highlight the fact that the nature of the managed risks varies. Risk is defined in ISO 31000 as the "*effect of uncertainty on objectives*," and it is specified in note 2 of this definition that "*Objectives can have different aspects and categories, and can be applied at different levels.*" Objectives can be financial, quality, information security, and at different levels: service, product, project, and process. In ISO 31000 and in our approach, the overall mechanisms of the practices for managing risks are not varying and follow principles of a management system environment. In our case, the management system mechanisms are not used for prescriptive aspects required by a management system certification but for integration and interoperability purposes. So, we completed our set of ISO standards with the ISO High Level Structure (HLS)[12] for management systems. The consensus previously mentioned is also true for an established common vocabulary regarding the main tackled concepts in project management, quality management, ITSM, and information security management. According to the authors experience and gained feedback from various R&D projects with companies in several domains, these topics are the most commonly addressed by many IT organizations, whatever their size and domain. To address these concerns with an operational approach for risk management and the varied nature of risks, we investigated the following research question: "*how to integrate risk management in IT organizations within a management system context?*"

The objective of this research is to propose means to improve Risk management processes in IT organizations, with a structured, integrated, interoperable, assessable, effective, and efficient way (these criteria guide our applied research). Then, we intend to propose a PRM and a PAM (also quoted as Process Models in the paper) as artifacts enabling process assessment and improvement. Both artifacts consolidate ISO standards which are already process oriented (ie, ISO 31000) but not structured neither organized for rigorous process assessment. So, this paper presents how we initiated the development of a PRM and a PAM for Integrated Risk Management in IT Settings (named IRMIS), by eliciting processes from the various ISO standards previously mentioned or from other ones derived from them and how we derived and described them in a systematic way. The approach relies on previous works which enabled to deploy successfully a Transformation Process[13] for designing PRMs and PAMs fulfilling the Process Assessment ISO standard requirements for developing PRMs and PAMs.[14] The ISO/IEC 27005[15] for Information security risk management is also of great help for dedicated Risk management processes, as well as the ISO 21500 for project management, proposing several processes covering Risk management activities.

The paper firstly presents in Section 2 some related works, and in Section 3, terminology concerning the main concepts of an Integrated Risk Management Process Model in IT organizations. Section 4 describes the methodology followed for building the process models, eliciting the processes with the proposition of a process map, and for describing processes with views derived from relevant selected ISO standards. Section 5 presents discussions before conclusions given in Section 6.

2 | RELATED WORK

Even being a key element, Integrated risk management has not been specifically addressed from the IT organizations point of view. Integrated risk management addresses risks at very different levels in the organization, including strategy and tactics, and covering both opportunity and threat.[16]

Diverse frameworks and approaches to support Integrated risk management in IT companies have been developed. A framework for the assessment and management of risk associated with the software development process was proposed by Chittister and Haimes.[17] The role of human resource development and improvement in risk assessment is given special attention. The framework from Lyytinen et al[18] synthesizes, refines, and extends different approaches to managing software risks. After exploring the environment of IT in companies and identifying the common threats, Bandyopadhyay et al[19] developed a framework with four major components: risk identification, risk analysis, risk-reducing measures, and risk monitoring. Riskit, a method developed by Kontio,[20] complements other risk management approaches by supporting qualitative and structured analysis of risks through a graphical modeling formalism. Together with the method, Kontio also proposed a risk management improvement framework that favors continuous and systematic improvement of the risk management process. Roy[21] developed the ProRisk Management Framework, which is intended to account for a number of the key risk management principles needed to manage the software development process. Attention in this framework is focused on the business domain in which the project is created, and the operational domain where the project is actually carried out. The Risk Management Framework from SEI[22] provides a comprehensive risk management methodology basis for the evaluation and the improvement of a program's risk management practice. It can be applied to support the management of different types of risk, such as software development risk, acquisition program risk, operational risk or information security risk. In addition, some studies[23] have identified the most useful components from diverse maturity models in order to guide the achievement of higher organizational maturity and capability levels. This approach has been used in Risk management maturity models with unification of practices and integrated multiple views. In the software domain, improvements are proposed in Buglione et al[23] for the Risk management process of the PAM ISO/IEC 15504-5.[24] Recently, a development of a Maturity Model for risk management has been performed,[25] based on the ISO 31000 standard version of 2009. The paper is proposing an analysis of existing maturity models related to risk management; the authors selected some inputs (ie, in CMMI) for structuring their proposed maturity model based on ISO 31000:2009. This maturity model addresses directly the ISO 31000 standard but is creating its own framework; it is not meeting ISO/IEC 330xx requirements for process capability and maturity assessment and does not address our research.

Information technology (IT) has become crucial in the digital era, and more and more threats are existing. Organizations have to face risks with appropriate approaches depending on their size. Despite the fact there are numerous risk management standards, few of them are integrated and adapted to small and medium sizes enterprises. A research proposes a comprehensive people, process, and technology application model for Information Systems risk management in small/medium enterprises.[26] These research works provide an interesting operational approach with operational aspects that can help describing best practices in a process model. From the project management perspective, a recent survey on ISO 21500 and PMBoK[27] has shown that quality management and risk management are the last processes to be considered by project managers. Risk management needs to be strengthened and adapted so that it is applied to the size and context of the company and multiple risk management frameworks can be exploited. In addition, Öbrand et al[28] investigated risk management from a performative perspective and showed how IT risks are addressed in a narrow sense, then contemporary organizations need to develop adaptive and reflexive capabilities.

In the IT domain, software engineering plays a significant part where risk management is also considered from various perspectives: embedded in project management, included in software process improvement (SPI) approaches or part of software and/or system life cycle. The SPI Manifesto[29] "*gives expression to state-of-the-art knowledge on SPI*" with three values (people, business, change), further elaborated into 10 principles including risk management. Risk management must be a part of any SPI project, and SPI risks must be managed as in any project. For software and system developments, risks management must be present. There is an ISO standard favoring risk management in life cycle processes: ISO/IEC/IEEE 16085[30]: "*This document provides a unified treatment of the processes and products involved in risk management throughout the life cycle of systems and software. It provides details for the management of risk in the context of system and software engineering.*" It is aligned with ISO 31000 and even if it does not require a management system, it is compatible with the quality management system of ISO 9001, the service management one of ISO/IEC 20000-1, and the information security one of ISO/IEC 27001. By doing so, it encourages a process approach with management system mechanisms. This standard is an inventory of other standards related to process life cycle and align terminology. But it does not provide a dedicated software view as many principles are similar to the generic risk management aspects depicted in ISO 31000.

In the C&MM landscape, process model engineering has been questioned many times in the literature. Some studies show some shortcomings in the development of such models.[31] Becker et al explored various C&MM[32] and Pöppelbuß some design principles for useful maturity models.[33] As the Capability Maturity Model was first developed in the Software engineering community and as the Process Assessment have its own ISO standard[5] with requirements for developing PRMs and PAMs,[14] different process models were developed in this area. A Brazilian initiative developed a framework for engineering process models in the software domain.[34] In the same vein, another Austrian initiative developed methodological support.[35] Several process models for IT and non-IT works have been developed in Luxembourg, in an R&D initiative encompassing the TIPA Framework[36] with PRMs and PAMs for ITIL and Operational risks.[37]

The integration of management systems, in particular from the ISO 9001 perspective, has been considered in many works. The latest ISO survey[38] shows that ISO/IEC 20000-1 and ISO/IEC 27001 remain the flagship standards in IT organizations. Haufe et al investigated what processes could be identified for an information security management system in Haufe et al[39] and propose a process framework based on a set of agreed upon ISMS processes in existing standards like ISO/IEC 27000 series, COBIT and ITIL. Authors confirmed that "*a process-oriented view of the ISMS [Information Security Management System] can help focusing on the operation of an ISMS and improve the efficiency while planning such processes. By this, as a main finding, the systemic character of the ISMS consisting of processes … is strengthened.*" The ISO standard ISO/IEC 27013[40] also proposes "*Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*" in order to help organizations implement ISO/IEC 27001 when ISO/IEC 20000-1 is already implemented or vice versa, implement both ISO/IEC 27001 and ISO/IEC 20000-1 together, or integrate existing management systems based on ISO/IEC 27001 and ISO/IEC 20000-1.

From a performance assessment perspective, the help of C&MM and assessment approaches has been demonstrated (with the CMMI and ISO/IEC 15504-33000 series of process models). In ISO, development works have proposed PRMs and PAM based on MSSs. This is the case for Information security management (ISO/IEC 33072[41]), for ITSM (ISO/IEC 15504-8[3]) and for quality management based on ISO 9001 (ISO/IEC 33073[42]). These three domains are of particular interest, as they propose from a generic perspective, a common set of processes addressing the management system mechanisms, as stated in the HLS for management systems. In the medical IT networks domain incorporating medical devices, some research and standardization works have been performed. A PRM and a PAM have been developed enabling risk management improvement. Healthcare Delivery Organizations can assess risk management process capability considering the requirements of IEC 80000-1 which is the application of risk management to IT-networks.[43] This risk management life cycle process model provides specific risk management processes in the medical sector. After some feedback on the barriers preventing the adoption of the standard, a new approach for simplifying the standard usage has been proposed for its revision. This approach is putting forward the idea of using the ISO Annex SL providing a HLS for management systems as a means to favor a process approach and management system mechanisms, reproducing the way we have proposed in our previous work.

Harmonization is crucial in organizations with multiple models at their different hierarchical levels. Having a great diversity of models involves a wide heterogeneity in the structure of the process entities and quality systems, and also in the organizational terminology.[44] The recent proliferation of language and terms usage in the software development domain has some implications for assessors and assessment frameworks, and for the broader community. In order to clarify as much as possible the language in this research, next section analyzes and settles the terminology that has been used.

3 | ISO BACKGROUND: TARGETED ISO STANDARDS AND TERMINOLOGY

In previous works, the authors explored risk management in IT organizations from the angle of selected relevant ISO standards with ISO 31000 as main theme. Table 1 provides the full list with identification numbers and titles of each selected standard, with the year of publication. It is important to quote that ISO 31000 has been republished at the beginning of 2018 and we consider this latest version for our R&D works, meaning a revision of previous works for encompassing changes (the main changes of this version reflect simplification and harmonization of terms and sentences for a generic risk management perspective, and a few changes in the overall Risk management process, such as the addition of the Recording and reporting sub-process; the mindset of the standard is open, without prescriptive elements for a free organization of risk management principles and activities; some definitions have been removed compared with the previous version, because they are already part of the ISO Guide 73[45]).

There are key concepts conveyed by these standards. We are paying a particular attention to the ones provided by the ISO 31000 as our main reference and checking shared used concepts with other standards we target in our works. Therefore, terms and definitions provided by ISO standards are our basis.

To start with, we remind the definition of **Risk** in ISO 31000 stating it is the "*effect of uncertainty on objectives*" (an objective being a result to be achieved). In ISO Annex SL, Risk is defined as "*effect of uncertainty*." ISO 9000 defines Risk as the "*effect of uncertainty on an expected result*." ISO/IEC 20000-10[46] and ISO/IEC 27000[47] have the same definition as ISO 31000. The only definition proposed by ISO 21500 regarding Risk is "*Risk register: record of identified risks*," including results of analysis and planned responses. We consider the selected standards are aligned for the term Risk.

Related to the Risk management terms, most definitions of ISO 31000 come from the ISO Guide 73:2009.[45] **Risk management** is defined as: "*coordinated activities to direct and control an organization with regard to risk*." The overall Risk management process described in ISO 31000 is part of a **context** (whether internal or external) defined in ISO 31000 as the "*environment in which the organization seeks to achieve its objectives*." This notion of context is present in management systems such as ISO 9001, ISO/IEC 20000-1, and ISO/IEC 27001, driven by the Annex SL dedicated clause on the "*context of the organization*." ISO 9000 specifically defines the context of the organization as "*business environment; combination of internal and external factors and conditions that can have an effect on an organization*'s." ISO 21500 proposes a clause on "*project environment*" stating that "*factors outside and inside the organization boundary may impact the project performance*." We consider the selected standards have a common meaning for the terms Context and Environment, but we favor the term Context which is shared between ISO 31000 and MSSs.

ISO 31000 does not dedicate a definition for the terms **Communication and consultation** (ISO 31000 states "Best available information" in the foundation principles for managing risks) but ISO Guide 73 does: "*continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk*." ISO/IEC 27000 (Overview and vocabulary) has exactly the same definition. In ISO 9000 (Fundamentals and vocabulary), Communication is not a defined term but is one of the fundamental principles specified as follows: "*Effective communication throughout the organization and relevant interested parties enhances involvement through better understanding of: the management system and its performance, and organizational values, objectives and strategies*." In ISO/IEC 20000-10, there is no definition for Communication nor for Consultation. We consider that the relevant definition of Communication and consultation for our works is the one from ISO Guide 73.

Monitoring: "*continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected*" and **Review**: "*activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives*" are both definitions in the ISO Guide 73, to be applied in ISO 31000. Annex SL and ISO 9000 define Monitoring as: "*determining the status of a system, a process or an activity*." ISO 9000 defines Review as: "*determination of the suitability, adequacy or effectiveness of an object to achieve established objectives*." ISO/IEC 27000 defines Review as in ISO 31000. ISO 20000-10 does not define Review but defines Monitoring as: "*determining the status of a system, a process or an activity*." We consider the selected standards have a common meaning for the terms Monitoring and Review.

Regarding the overall risk management process, we can also precise key concepts which are defined in the ISO Guide 73 and some of them in ISO 21500 for the following sub-processes of risk management in both ISO 31000 and ISO 21500:

- **Risk assessment**: in ISO Guide 73, it is defined as the "overall process of risk identification, risk analysis and risk evaluation."
- **Risk identification**: in ISO Guide 73, it is defined as the "process of finding, recognizing and describing risks"; ISO 21500 states the purpose of Identify risks process is "to determine potential risk events and their characteristics that, if they occur, may have a positive or negative impact on the project objectives."

TABLE 1 List of selected ISO standards for exploring risk management

ISO Standard Number	ISO Standard Title
ISO 31000:2018	Principles and generic guidelines on risk management
ISO annex SL: 2018	Proposals for management system standards (in ISO/IEC directives, part 1, consolidated ISO supplement)
ISO 9001:2015	Quality management systems—Requirements
ISO 21500:2012	Guidance on project management
ISO/IEC FDIS 20000-1:2018	Information technology—service management—part 1: Service management systems requirements
ISO/IEC 27001:2013	Information technology—security techniques—information security management systems—requirements

- **Risk analysis:**in ISO Guide 73, it is defined as the "process to comprehend the nature of risk and to determine the level of risk";
- **Risk evaluation**: in ISO Guide 73, it is defined as the "process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable"; ISO 21500 states the purpose of Assess risks process is "to measure and prioritize the risks for further action."
- **Risk treatment**: in ISO Guide 73, it is defined as the "process to modify risk." ISO 21500 states the purpose of Treat risks process is "to develop options and determine actions to enhance opportunities and reduce threats to project objectives."

We can see that the terminology is not completely aligned between ISO Guide 73, ISO 31000, and ISO 21500 with differences related to the use of "*assess*," "*analyze*," and "*evaluate*," even if the global risk assessment from the ISO 31000 perspective is similar. The latest version of ISO 31000 intends to propose an harmonized vocabulary which can be adopted easily in all domains of risks and all standards tackling the concepts of Risk. It is generally easy to make the correspondence via synonyms. For instance, "*residual risks*" is now "*remaining risks*" in ISO 31000; "*likelihood*" is favored to "*probability*" because of its broader sense in English; "*consequence*" is used rather than "*impact*."

From a systemic perspective (as embraced in management systems in general), we can see the Risk management overall process is part of a global framework. Some general definitions related to governance and management are then of particular interest. We can quote Leadership and commitment in ISO 31000; also, we find Leadership and commitment in Annex SL and MSS such as ISO 9001, ISO/IEC 20000-1, and ISO/IEC 27001, and Project Governance and Organization in ISO 21500. These terms are not defined in these standards, but there have common defined aspects. Another term we tackle is **Stakeholder**, defined in ISO 31000 as "*person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity*." It is exactly the same definition in Annex SL, so it is aligned for all selected MSSs. And ISO 21500 has a concept akin to the project object: "*person, group or organization that has interests in, or can affect, be affected by, or perceive itself to be affected by, any aspect of the project*." Another aspect is **Risk management policy**, no longer defined in ISO 31000 but defined in ISO Guide 73 in the context of risk management as follows: "*statement of the overall intentions and direction of an organization related to risk management*," and in Annex SL: "*intentions and direction of an organization, as formally expressed by its top management"* (so it is aligned for all selected MSSs). And finally **Top management**, not defined in ISO 31000, but important from the management perspective of any system, dedicated to risk or other; Annex SL defines it as "*person or group of people who directs and controls an organization at the highest level*" (all selected MSS are aligned with this definition, even if there are slight differences due to the targeted domain in ISO/IEC 20000-1 mentioning explicitly "service"). Policy and Top management terms are not used in ISO 21500.

Documented information is also a common concern, even if not defined specifically in ISO 31000, but referred to and used from policy and reporting perspectives. We can quote Annex SL definition: "*information required to be controlled and maintained by an organization and the medium on which it is contained*." This definition can apply for all selected standards.

Finally, **Continual improvement** is a concept in the quality loop related to the risk management framework. These terms are not defined in ISO 31000 neither in the ISO Guide 73, but Continual improvement is considered as a key attribute for enhanced risk management in ISO 31000. Continual improvement terms are defined in Annex SL as: "*recurring activity to enhance performance*." This definition can apply for all selected standards.

In addition to Risk management concepts, Management systems ones play an important part from an integrated risk management perspective. The terms we went through in this section will be used as reference points in the next section of the paper.

4 | THE IT ORGANIZATIONS INTEGRATED RISK MANAGEMENT PROCESS MODEL DEVELOPMENT: HOW TO IDENTIFY AND DESCRIBE PROCESSES?

In order to design and build process models providing a solution for the research question, artifacts have been created for an Integrated Risk Management for IT Settings (IRMIS) PRM and PAM. A Design Science Research method has been followed, as reported in Barafort et al.[48] For the Build part of the Design Science Research method, the authors have met the requirements of ISO/IEC 33004[14] for designing PRMs and PAMs. They have also used a Transformation Process.[13] This process is a systematic approach, based on goal-oriented requirements engineering techniques, for designing PRMs and PAMs. It contains nine steps described in detail in Barafort et al[13]; these steps are the following: (1) Identify elementary statements in a collection of statements (in Barafort et al[13] we have used "requirements" as a generic term. In the context of the various selected ISO standards of our research, we talk about "statements" and use this term equally); (2) Organize and structure the statements; (3) Identify common purposes upon those statements and organize them; (4) Identify and factorize outcomes from the common purposes and attach them to the related goals; (5) Group activities together under a practice and attach it to the related outcomes; (6) Allocate each practice to a specific capability level; (7) Phrase outcomes and process purpose; (8) Phrase the Base Practices attached to Outcomes; and (9) Determine Work Products among the inputs and outputs of the practices.

This Transformation Process has been used successfully several times and validated in the context of the TIPA Framework.[36] With the building of PRM and PAM, we aim at satisfying a set of criteria for the produced models, as detailed in Barafort et al.[49] These criteria are considered during the building of IRMIS PRM and PAM, with Integration as the key one. They are the following:

- Integration: the expected PRM and PAM need to facilitate the integration of risk management between multiple frameworks and management systems. For that, the produced PRM and PAM describe generic aspects for the risk management framework, aligned with common/generic parts of any management system (namely the Annex SL) and with a few terms adapted to a risk management framework as stated in ISO 31000, plus risk management dedicated aspects derived from ISO 31000.

- Assessability: each process is described in a way that facilitates its future assessment: each process has one single purpose; the process outcomes are necessary and sufficient to achieve the process purpose; each process outcome is defined as a measurable objective; the base practices reflect the process purpose and outcomes.
- Interoperability: the produced model describes processes and work products in a way that fosters the exchanges between the risk management framework and several management systems.
- Completeness: the expected process models need to address all concepts contained in ISO 31000. For that, the traceability between the clauses of ISO 31000 and the processes contained in the produced process assessment model are ensured.
- Adoption: the produced process models need to describe the processes in a way that encourages the adoption of these processes. For that, the proposed processes are designed in a way that reflects the terminology of risk management and of a system of processes, as found in a risk management framework advocated by ISO 31000.
- Applicability: The proposed PRM and PAM need to fit in with all companies, regardless of their type, size, or nature. They need to be usable for various purposes such as: the rating and capability determination of an individual process, the determination of the organizational maturity, the preparation for audit, or benchmarking. For that, the produced process models are designed in a way that ensures its compliance with all the requirements of ISO/IEC 33004.[14]

In this paper, we explain how we went through the Transformation process and when needed additional mappings in order to provide full process descriptions based on ISO 31000, and complementary views for ISO 21500 and ISO/IEC 27001 (completed with ISO/IEC 27005) as these standards provide inputs for specific risk management processes. ISO 9001 and ISO/IEC 20000-1 are not long-winded on risk management and are very aligned with Annex SL.

4.1 | Identification of elementary statements from ISO 31000

This step consisted in identifying all of the statements from ISO 31000 under the form of a collection of elementary items. The final list was composed of 281 elementary items made up of a subject, a verb, and a complement, without coordination, conjunctions, or enumeration. Table 2 shows an example of decomposed elementary requirements (when the latest version of ISO 31000 has been published, the identification of all the statements was redone from scratch). Then, from this final list, the “should statements” (main statements) contained in the text of the ISO 31000 standard were easily identified (172 “should” statements). They are the basis for the next steps.

4.2 | Organization and structure of the statements

A “mind map” for statement trees organized and structured the elementary “should” statements, completed by “info” statements (74), “may” statements (16), “can” statements (24), “purpose” statements (9), and other statements (7). A graphical view of the elementary items having the same object (or component) was provided. The requirements were then gathered around the objects they were relating to in order to build statement trees. A decision was sometimes made to distribute in various statement trees the set of statements; this was guided by the affiliation of statements within Clauses. These trees considered the Clauses and Sub-clauses titles, as well as the subject of each elementary item. For instance, elementary items targeting “context” aspects were grouped under an “External and internal context” label. This statement tree structuring was inspired by previous works on the Annex SL for Management Systems Standards,[50] where some groupings were similar, and by mappings performed on the Risk term in the various selected standards. Therefore, related to the statements establishing the overall framework of risk management, we identified a Statement tree named *Leadership*, which has the following nodes (each node comprising leaves where each leaf is an elementary statement): Needs of the organization, Top management and oversight bodies commitment, Accountabilities-responsibilities-authorities, External and internal context, Risk management integration, and Scope definition. The other following statement trees were developed: *Communication and reporting*, *Resources*, *Implementing risk management*, *Risk assessment*, *Risk treatment*, and *Monitoring and review*. Finally, with the integration criteria, the Statement trees developed by the authors for the HLS of management systems were superimposed for relevant similar items, guided by terminology and common meanings. For instance in the Leadership tree, “Leadership and commitment” clause in ISO 31000, represented in a leaf was superimposed with “Leadership and commitment” clause of the HLS.

TABLE 2 Example of decomposed elementary statements

4.3.2 Extract from ISO 31000	Example of DecomposedElementary Statements
The organization should continually improve the suitability, adequacy and effectiveness of the risk management framework and the way the risk management process is integrated.	The organization should continually improve the suitability, adequacy and effectiveness of the risk management framework The organization should continually improve the way the risk management process is integrated.

4.3 | Identification and organization of common purposes

With the identification and organization of common purposes, a first list of elicited processes appeared, for an integrated risk management PRM. Each pre-identified process was represented as a goal tree with some logical grouping of common purposes. For each low-level objective within each goal tree, there is an elementary statement of the ISO standard. In addition to the Transformation Process, which has been followed for previous PRMs and PAMs development, we used low-level objectives resulting from the HLS and superimposed them with those from ISO 31000 in order to cover the common purposes of all the selected ISO MSSs for an integrated risk management PRM. The six key criteria listed at the beginning of this section were kept in mind, and particularly the integration and adoption ones, analyzed from the process selection perspective: ISO 31000 is a non-prescriptive standard but some good practices from Management standards such as ISO/IEC 27001 can be kept in order to ensure a better integration with MSSs (for example, the notion of policy is only suggested in ISO 31000: we believe it is part of best practices to develop such a policy); some wording of ISO 31000 is also kept in order to align on the best way on ISO 31000: the notion of Risk Management Framework with this wording is kept for not "forcing" minds to have a MSS vocabulary at all costs.

The Granularity level is another criterion to keep in mind: not to have too many processes, but with the objective to facilitate integration and interoperability of processes.

Figure 1 shows the goal tree for the *Leadership* process, containing six different objectives, resulting into five outcomes identified from the core common process Leadership of Annex SL, present for instance in the ISO/IEC 33073 standard for Quality Management System (for our ISO 31000 PRM & PAM design objective, "management system" and "quality management" have been, respectively, changed by "risk management framework" and "risk management").

In parallel and in order to help the identification of common purposes and processes, based on Statement trees performed in step 2, supported by the terminological work described in Section 3, by previous works at the ISO for developing PRMs and PAMs based on ISO/IEC 20000-1, ISO/IEC 27001, and currently ISO 9001, a mapping was performed. It was between the subclauses of ISO 31000, and the process names of MSSs common processes related to the core processes of a management system (the source document for the mapping with common processes for MSS was the ISO/IEC 33073 for the process capability assessment model for quality management). We insist here on the fact that the framework for risk management of the ISO 31000 shares the concepts of management systems (without seeking for a certification). This mapping also comprised the processes of ISO 21500. The mapping contributed to the identification of common purposes which are formulated into Goal trees (like in Figure 1) and to derive a first list of processes, to be refined (see Table 3).

Considering the Risk Management process viewed from ISO 31000 perspective, the "*Risk and opportunity management*" process proposed by PRM and PAM for Management Systems is not satisfactory. Indeed, it does not provide the necessary structure and details that we expect for a dedicated Risk Management PRM and PAM. As shown in our previous work,[6] ISO 21500 proposes a subject group dedicated to Risk management, with four processes: Identify risks, Assess risks, Treat risks, and Control risks. These four processes support our idea for having the overall Risk management process split into more detailed ones. In order to strengthen the approach, we used another ISO standard: the ISO/IEC 27005 Information security risk management. This standard is fully aligned with ISO 31000 and provides a more detailed view for the Information security domain. A mapping was performed between the subclauses of ISO 31000 and clauses and subclauses of ISO/IEC 27005. It confirmed our view for targeting Risk identification, Risk analysis, Risk evaluation and Risk treatment. Here is an extract of this mapping in Table 4.

Considering our approach for identifying elementary statements, grouping them in Statements trees, identifying common purposes and organizing them in Goal trees, completed by some mappings of clauses and subclauses of ISO 31000 with various ISO standards, the following list of processes is proposed in Figure 2 for an IRMIS Process Model in IT organizations. The IRMIS process model is composed of three groups of processes: Top Management, Common processes, and Risk management (see Figure 2). This structure with three groups is similar to the one of management systems including top management, and core common processes. Top Management and Common processes are mainly derived from the ISO/IEC 33073 standard[42] which is the latest version of a PAM published by ISO; only two processes are derived from ISO/IEC 33072[41] for

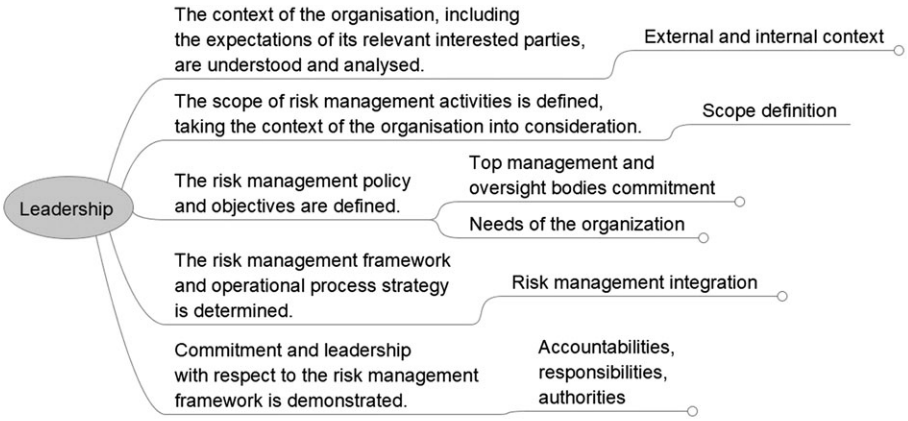
Leadership
The context of the organisation, including the expectations of its relevant interested parties, are understood and analysed.
External and internal context
The scope of risk management activities is defined, taking the context of the organisation into consideration.
Scope definition
The risk management policy and objectives are defined.
Top management and oversight bodies commitment
Needs of the organization
The risk management framework and operational process strategy is determined.
Risk management integration
Commitment and leadership with respect to the risk management framework is demonstrated.
Accountabilities, responsibilities, authorities

FIGURE 1 Goal tree for the leadership process

TABLE 3 Mapping between ISO 31000 subclauses and common processes of MSSs

ISO 31000:2018 Subclauses	ISO/IEC 33073 PRM with Common Processes for MSS	Proposed Processes for IRMIS PRM
5.2 Leadership and commitment	TOP.1 Leadership	Leadership
5.3 Integration	COM.08 Operational planning	Operational planning
5.4.1 Understanding the organization and its context	TOP.1 Leadership	Leadership
5.4.2 Articulating risk management commitment	TOP.1 Leadership	Leadership
5.4.3 Assigning organizational roles, authorities, responsibilities, and accountabilities	TOP.1 leadership	Leadership
5.4.4 Allocating resources	COM.03 Human resource management	Resource management
5.4.5 Establishing communication and consultation 6.2 Communication and consultation	COM.01 Communication management	Communication management
Notions of documents	COM.02 Documentation management	Documentation management
5.5 Implementation	COM.09 Operational implementation and control	Operational implementation and control
5.6 Evaluation (NEW)	COM.10 Performance evaluation	Performance evaluation
5.7 Improvement	COM.04 Improvement	Improvement
No “audit” notion in 31000	COM.05 Internal audit	
No “non-conformity” notion in 31000	COM.07 Non-conformity management	
6.3.2 Defining the scope	TOP.1 Leadership	Leadership
6.3.3 External and internal context	TOP.1 Leadership	Leadership
6.3.4 Defining risk criteria		Defining risk criteria
6.4.2 Risk identification	COM.11 Risk and opportunity management	Risk identification
6.4.3 Risk analysis		Risk analysis
6.4.4 Risk evaluation		Risk evaluation
6.5 Risk treatment		Risk treatment
6.6 Monitoring and review	COM.06 Management review	Review Monitoring
6.7 Recording and reporting (NEW)		Recording and reporting

TABLE 4 Mapping of subclauses of ISO 31000:2018 and ISO/IEC 27005

ISO 31000	ISO/IEC 27005
6.1 General	
6.2 Communication and consultation	11. Information security risk communication and consultation
6.3.1 Establishing the context—general	7. Context establishment
6.4 Risk assessment	8. Information security risk assessment
6.4.1 General	8.1 General description of information security risk assessment
6.4.2 Risk identification	8.2 Risk identification
	8.2.1 Introduction to risk identification
	8.2.2 Identification of assets
	Annex B Identification and valuation of assets and impact assessment
	8.2.3 Identification of threats
	Annex C Examples of typical threats
	8.2.4 Identification of existing controls
	8.2.5 Identification of vulnerabilities
	Annex D Vulnerabilities and methods for vulnerability assessment
	8.2.6 Identification of consequences
6.4.3 Risk analysis	8.3 Risk analysis
	Annex E Information security risk assessment approaches
	8.3.1 Risk analysis methodologies
	8.3.2 Assessment of consequences
	8.3.3 Assessment of incident likelihood
	8.3.4 Level of risk determination
6.4.4 Risk evaluation	8.4 Risk evaluation

(Continues)

TABLE 4 (Continued)

ISO 31000	ISO/IEC 27005
6.5 Risk treatment	9 Information security risk treatment
6.5.1 General	9.1 General description of risk treatment
6.5.2 Selection of risk treatment options 6.5.3 Preparing and implementing risk treatment plans	9.2 Risk modification Annex F Constraints for risk modification 9.3 Risk retention 9.4 Risk avoidance 9.5 Risk sharing
6.7 Recording and reporting	10 Information security risk acceptance
6.6 Monitoring and review	12 Information security risk monitoring and review
	12.1 Monitoring and review of risk factors
5.7 Improvement	12.2 Risk management monitoring, review and improvement

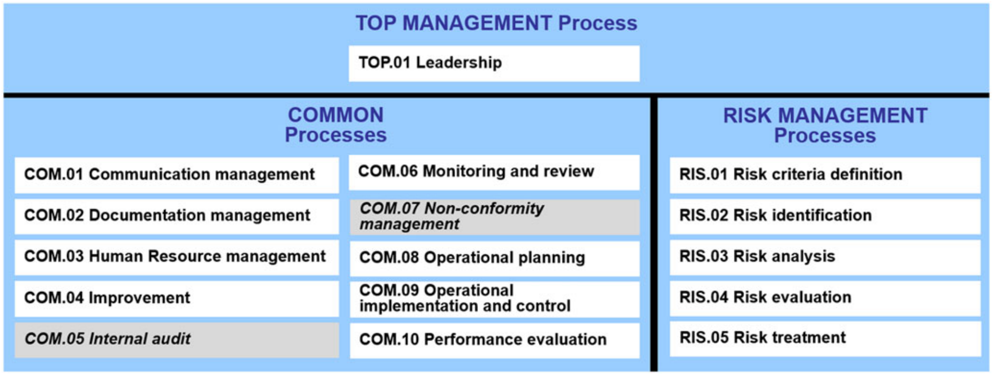
TOP MANAGEMENT Process
TOP.01 Leadership
COMMON Processes
COM.01 Communication management
COM.02 Documentation management
COM.03 Human Resource management
COM.04 Improvement
COM.05 Internal audit
COM.06 Monitoring and review
COM.07 Non-conformity management
COM.08 Operational planning
COM.09 Operational implementation and control
COM.10 Performance evaluation
RISK MANAGEMENT Processes
RIS.01 Risk criteria definition
RIS.02 Risk identification
RIS.03 Risk analysis
RIS.04 Risk evaluation
RIS.05 Risk treatment

FIGURE 2 IRMIS PRM proposed list of processes

COM.08 and COM.09 as there were two quality management dedicated; a more generic process description from ISO/IEC 33072 was then chosen. The Risk management group represents the specific processes for risk management, aligned with the overall risk management process proposed by ISO 31000.

Remark: the gray cells with italic texts show two processes which are not at all present in ISO 31000, but necessary in a management system context according to Annex SL; we decided to leave them in the PRM and PAM for global integration purposes.

4.4 | Identification and phrasing of outcomes and purpose

Common purposes were identified by grouping statements. Then, it enabled to formulate outcomes according to ISO/IEC 33004 requirements (An outcome is an observable result of (1) "*the production of an artefact*," (2) "*a significant change of state*," or (3) "*the meeting of specified constraints*."). For instance, for the Leadership process, this step was shortened by mapping the goal tree with the outcome of the core common Leadership process of the MSS (ie, in ISO/IEC 33073). The process description is then simplified and straightforward as long as grouping of elementary statements are mapped with outcomes of the MSS-based process. For Risk management specific processes, outcomes were identified and phrased from the grouping of elementary statements as common purposes with fulfilling ISO/IEC 33004 requirements above-mentioned. Then, from the phrased outcomes, a purpose for each process has been formulated. Table 5 lists the process purposes for each process, and the main source for the process description.

4.5 | Determination of indicators such as base practices and work products

In ISO 31000, sometimes the statements are detailed enough and can be the source of information for phrasing base practices; sometimes, there are not detailed. In that case, practices are directly deduced from the outcomes and represent functional activities of the process, with the adequate phrasing starting with an action verb at the infinitive. Each base practice must contribute to at least one outcome and must not contribute to capability levels upper than 1; they are phrased as actions.

The artifacts associated with the execution of a process are work products. Input and output work products are indicative and not exhaustive.

The selected measurement framework of IRMIS PAM is based on the process measurement framework for process capability assessment proposed in ISO/IEC 33020.

TABLE 5 Process ID, name, purpose, and main source document of the IRMIS PAM processes

Process ID and Name	Process Purpose	Main Source Document
TOP.01 Leadership	The purpose of leadership is to direct the organization in the achievement of its vision, mission, strategy, and goals, through assuring the definition of a management framework, a management framework policy, and management framework objectives.	ISO/IEC 33073
COM.01 Communication management	The purpose of communication management is to produce timely and accurate information products to support effective communication and decision making.	ISO/IEC 33073
COM.02 Documentation management	The purpose of documentation management is to provide relevant, timely, complete, valid documented information to designated parties.	ISO/IEC 33073
COM.03 Human resource management	The purpose of human resource management is to provide the organization with necessary competent human resources and to improve their competencies, in alignment with business needs.	ISO/IEC 33073
COM.04 Improvement	The purpose of improvement is to continually improve the risk management framework and its processes.	ISO/IEC 33073
COM.05 internal audit	The purpose of internal audit is to independently determine conformity of the management framework, products, services, and processes to the requirements, policies, plans, and agreements, as appropriate.	ISO/IEC 33073
COM.06 Monitoring and review	The purpose of monitoring and review process is to assess the performance of the risk management framework, to identify, and make decisions regarding potential improvements.	ISO/IEC 33073
COM.07 Non-conformity management	The purpose of the non-conformity management process is to resolve non-conformities and to eliminate their causes when appropriate.	ISO/IEC 33073
COM.08 Operational planning	The purpose of operational planning is to define the characteristics of all operational and organizational processes, and to plan their execution.	ISO/IEC 33072
COM.09 Operational implementation and control	The purpose of the process implementation and control process is to deploy and control the execution and performance of operational and organizational processes.	ISO/IEC 33072
COM.10 Performance evaluation	The purpose of performance evaluation is to collect and analyze data that will be used to evaluate the performance of the management framework and the business processes in terms of the defined objectives.	ISO/IEC 33073
RIS.01 Risk criteria definition	The purpose of the risk criteria definition process is to set and continually update risk criteria according to scope, context and objectives of the organization.	ISO 31000
RIS.02 Risk identification	The purpose of the risk identification process is to find and describe risks that might help or prevent an organization from achieving its objectives.	ISO 31000
RIS.03 Risk analysis	The purpose of risk analysis is to determine a level of risk from analysis techniques and factors of risks.	ISO 31000
RIS.04 Risk evaluation	The purpose of risk evaluation is to support decisions.	ISO 31000
RIS.05 Risk treatment	The purpose of risk treatment is to select and implement options for addressing risk.	ISO 31000

For core common processes deduced from ISO 31000 and quite similar to core common MSS ones, a mapping has been performed between goal trees, and existing process description in (ie) ISO/IEC 33073. The Management system terms are not reused as such but are replaced by ISO 31000 relevant ones: the main replacement concerns “management system,” replaced by “risk management framework,” as illustrated before with Leadership, and in the Improvement process description below (including Table 6 for the process description in the PAM).

4.6 | Improvement process description

Process ID COM.04

Name Improvement

Purpose The purpose of Improvement is to continually improve the risk management framework and its processes and its processes

Outcomes As a result of successful implementation of this process:

1. Opportunities for improvement are identified.
2. Opportunities for improvement are evaluated against defined criteria.
3. Improvements are prioritized.
4. Improvements are implemented.
5. The effectiveness of implemented improvements is evaluated.

TABLE 6 The improvement process description in the IRMIS PAM

	ISO 31000 View
Process ID	Com.04
Process name	Improvement
BP1 (out 1)	Identify improvement opportunities.
BP2 (out 2)	Evaluate improvement opportunities.
BP3 (out 3)	Prioritize improvements.
BP4 (out 4)	Implement improvements.
BP5 (out 5)	Evaluate improvements.
Input work products	Improvement opportunity approval request [outcome 5] Improvement opportunity evaluation criteria [outcome 2,4] Improvement opportunity evaluation result [outcome 3,4] Improvement opportunity record [outcome 2,3] Improvement policy [outcome 2] Improvement procedure [outcome 2,3] Improvement target [outcome 4,5]
Output work products	Improvement implementation schedule [outcome 4] Improvement opportunity [outcome 1] Improvement opportunity approval request [outcome 3] Improvement opportunity evaluation report [outcome 2] Improvement opportunity evaluation result [outcome 2] Improvement opportunity implementation log [outcome 5] Improvement opportunity record [outcome 1] Improvement target [outcome 3] Risk management framework strategy [outcome 1]

4.6.1 | Comments on the improvement process

This process is directly inspired from the Improvement process of the core common processes for a management system. The improvement mechanisms are sufficiently generic and can be applied to a risk management framework without particular adaptations. In the case of this process, no dedicated view is provided for ISO 21500 and ISO/IEC 27001 as there are no detailed statements related to improvement in these respective standards.

In order to provide a process illustration dedicated to Risk management, the Risk treatment process is proposed below. As mentioned previously in the paper, the activities at the heart of risk management are specifically described in the IRMIS PRM and PAM. Previous works have enabled to present Risk identification,[48] Risk analysis, and Risk evaluation.[49] We are now presenting Risk treatment derived from ISO 31000, with additional views providing information coming from ISO 21500 and ISO/IEC 27001 (see Table 7). We have made this deliberate choice because ISO 9001 and ISO/IEC 20000-1 do not provide detailed information related to Risk treatment, contrary to ISO 21500 and ISO/IEC 27001 (as well as inputs from ISO/IEC 27005).

4.7 | Risk treatment process description

Process ID RIS.05

Name Risk treatment

Purpose The purpose of risk treatment is to select and implement options for addressing risk.

Outcomes As a result of successful implementation of this process:

1. Risk treatment options are selected by balancing potential benefits against the costs, effort, or disadvantages of implementation.
2. Selected risk treatment options are specified with appropriate information for justification, implementation, integration, and documentation.
3. Risk treatment plans for remaining risks and new risks are executed.
4. Remaining risks are communicated to decision makers and other stakeholders.
5. Each risk change to consider is updated.

4.7.1 | Comments on the risk treatment process

This process is critical in the overall risk management loop. It is the process to modify risk (as defined in the ISO Guide 73). When treating risks, new risks can appear (and then, they have to be assessed), and existing risks are modified.

After designing the IRMIS PRM and PAM first drafts, a first level of validation has been performed by experts with knowledge in ISO/IEC 330xx, project management, ITSM, and Information security. A set of systematic review criteria has been used: an outcome is targeting capability

TABLE 7 The risk treatment process description and views in the IRMIS PAM

	ISO 31000 View	ISO 21500 View	ISO/IEC 27001 View
Process ID	RIS.02		
Process name	Risk identification		
BP1 (out 1)	Select risk treatment options. For selecting risk treatment options, consider the organization's objectives, risk criteria, and available resources.	Insertion of resources and activities into the budget and schedule	Selection of appropriate information security treatment options, taking into account of the risk assessment results
BP2 (out 2)	Specify selected risk treatment options with appropriate information for justification, implementation, integration, and documentation in a risk treatment plans.	Risk treatment includes measures to avoid the risk, to mitigate the risk, to deflect the risk, or to develop contingency plans to be used if the risk occurs	Formulate an information security risk treatment plan
BP3 (out 3)	Execute risk treatment plans for remaining risks and new risks.		Determine all controls that are necessary to implement the information security risk treatment options chosen
BP4 (out 4)	Communicate remaining risks to decision makers and other stakeholders.		Obtain risk owner's approval of the information security risk treatment plan and acceptance of the residual information security risks
BP5 (out 5)	Update risk changes in the risk register.		The organization shall retain documented information about the information security risk treatment process.
Input work products	Risk register Risk criteria	Risk register Project plans	Information security risk treatment plan
Output work products	Risk treatment plans Remaining risks Risk register	Risk responses Change requests Risk register	

level 1 only; an outcome can be identified as an artifact; the wording is clear and appropriate for all PAM components; the vocabulary used in the PAM is consistent; each process is defined with the characteristics presented at the beginning of the section: integration, assessability, interoperability, completeness, adoption, and applicability. Some improvements have been performed, particularly for the wording and the used terminology. All the processes of the PRM and PAM are reviewed on the same way.

5 | DISCUSSION

In this paper, the integration aspect is paramount. This is the reason why the integration based on terminology and structuring is essential. As ISO standards are developed on the basis of international consensus, the terminology equipping these standards is proven and recognized. On top of that, ISO has performed a dedicated effort for harmonizing Management System Standards by imposing a common structure for all of them, with compulsory clauses and requirements. Even if our main line is driven by ISO 31000 which is not identified "directly" as a management system (defined in Annex SL as a "*set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives*"), it is admitted that the risk management framework advocated by ISO 31000 ("*set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization*") is similar to a management system as defined in Annex SL (see above). The various mappings performed by the authors confirmed this. But the authors have chosen to name the system as "Risk management framework" in each place where "xxx management system" was used in the common processes described in existing PRM and PAM.[50] On the other hand, ISO 31000 being a guideline standard and not a requirements one, some identified processes labeled as "common processes" are not existing in ISO 31000 (no statements related to *Audit* neither *Non-conformity management*: their name is in italics in the process map). The authors chose to let them appear in the process map from an integration perspective with MSSs such as ISO 9001, ISO/IEC 27001, and ISO/IEC 20000-1.

From assessability and adoption perspectives, it is necessary to keep an adapted number of processes for a pragmatic and operational implementation in organizations. The process name has also to be clearly identified and understood by practitioners. The authors have made assumptions based on the current terminology of ISO 31000. For instance, the Review concept is not associated with the term Management in our proposed process models, and Monitoring is associated directly with Review; this is more adapted to the risk management context than to the MSS one. In the same logic, Evaluation from ISO 31000 is named Performance evaluation in ISO/IEC 33073, so we kept the same label Performance evaluation in our proposed process model.

When developing a process reference model, as stated in ISO/IEC 33004: "*process descriptions shall not contain or imply aspects of the process quality characteristics beyond the basic level of any relevant process measurement framework conformant with ISO/IEC 33003*." The fact to deal with documentation and planning aspects could be linked to Capability Level 2. In order to simplify and clarify alignment with statements, a dedicated process for Documentation management and a dedicated one for Operational planning have been identified. Documentation management was not identified as such in ISO 31000. But the authors decided to propose a dedicated process and to adopt the same documentation management mechanisms as the ones of this process in MSS PRM and PAM.

The IT organizations specificities are not particularly visible in the elicitation of processes at the PRM level. A particular attention is paid on these aspects at the PAM level in particular with the view provided for Information security with ISO/IEC 27001.

Finally, the risk management dedicated processes of the PRM are finding most of their inputs in ISO 31000, and ISO 21500, ISOIEC 27001, and ISO/IEC 27005 as complement in the IRMIS PAM. With the IT organizations mindset, specific concerns related to risk management remain connected with service management and information security, respectively, for ISO/IEC 20000-1 and ISO/IEC 27001.

6 | CONCLUSION AND NEXT STEPS

This paper describes the elicitation and description of processes for the construction of an IRMIS process model. For doing so, a Transformation Process has been applied, complemented by some mappings with supporting ISO standards. The resulting process model is covering the processes identified from ISO 31000, with common ones in MSS and in ISO 21500 because management system mechanisms are present in all of them, even if all standards are not enabling certification. In addition, more specific processes have been identified for the dedicated Risk management activities.

Because we consider that risk management organizational capabilities in companies with IT organizations can be strengthened by IRMIS processes based on selected ISO standards, a PRM and a PAM are aiming at equipping organizations for process assessment and improvement. The selected ISO standards were voluntarily empirically kept limited to the most significant ones in IT organizations (ie, ISO 31000, ISO 9001, ISO 21500, ISO/IEC 20000-1, and ISO/IEC 27001), and Annex SL has been used for supporting our approach. This paper describes the first iteration towards a full PRM and PAM with a proposition of elicited processes. More iterations to refine this process list will be performed, as well as experts' validation. Some field's experimentations can also contribute to the artifacts validation. Situational factors may also be investigated in order to check the best way to apply this generic and integrated Risk management process reference model in IT organizations.

ACKNOWLEDGEMENTS

This work has been supported by the Spanish Ministry of Science and Technology with ERDF funds under grants TIN2016-76956-C3-3-R.

ORCID

Antoni-Lluís Mesquida http://orcid.org/0000-0002-1191-6220

REFERENCES

1. Automotive Spice, http://www.automotivespice.com/fileadmin/software-download/Automotive_SPICE_PAM_30.pdf (online: accessed 20-May-2018) (2016)
2. TIPA for ITIL, https://www.list.lu/fileadmin//files/projects/TIPA_T10_ITIL_PAM_r2_v4.1.pdf (online: accessed 20-May-2018) (2015)
3. *ISO/IEC 15504-8: Information Technology—Process Assessment—An Exemplar Process Assessment Model for IT Service Management*. Geneva: International Organization for Standardization; 2012.
4. Lepmets M, McCaffery F, Clarke P. Development and benefits of MDevSPICE®, the medical device software process assessment framework. *Journal of Software: Evolution and Process*. 2016;28(9):800-816.
5. *ISO/IEC 33001: Information Technology—Process Assessment—Concepts and Terminology*. Geneva: International Organization for Standardization; 2015.
6. Barafort B, Mesquida AL, Mas A. Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces*. 2016.
7. *ISO 9001: Quality Management Systems—Requirements*. Geneva: International Organization for Standardization; 2015.
8. *ISO/IEC 27001: Information Technology—Security Techniques—Information Security Management Systems—Requirements*. Geneva: International Organization for Standardization; 2013.
9. *ISO/IEC FDIS 20000-1: Information Technology—Service ManagementvPart 1: Service Management System Requirements*. Geneva: International Organization for Standardization; 2018.
10. *ISO/IEC ISO 21500: Guidance on Project Management*. Geneva: International Organization for Standardization; 2012.
11. *ISO 31000: Risk Management—Principles and Guidelines*. Geneva: International Organization for Standardization; 2018.
12. *ISO/IEC Directives, Part1, Annex SL*. Geneva: International Organization for Standardization; 2018.
13. Barafort B, Renault A, Picard M, Cortina S. A transformation process for building PRMs and PAMs based on a collection of requirements—example with ISO/IEC 20000. 8th international SPICE 2008 conference, Nuremberg (2008)
14. *ISO/IEC 33004: Information Technology—Process Assessment—Requirements for Process Reference, Process Assessment and Maturity Models*. Geneva: International Organization for Standardization; 2015.

15. *ISO/IEC 27005: Information Technology—Security Techniques—Information Security Risk Management—Requirements*. Geneva: International Organization for Standardization; 2011.
16. David Hillson. Integrated risk management as a framework for organisational success. Proceedings of the PMI Global Congress 2006 North America, presented in Seattle WA, USA, 23 October (2006)
17. Chittister C, Haimes YY. Risk associated with software development: a holistic framework for assessment and management. *IEEE Transactions on Systems, Man, and Cybernetics*. 1993;23(3):710-723, May/June.
18. Lyytinen K, Mathiassen L, Ropponen J. A framework for software risk management. *Journal of Information Technology*. 11(4, 1996):275-285. (1996)
19. Bandyopadhyay K, Mykytyn PP, Mykytyn K. A framework for integrated risk management in information technology. *Management Decision*. 1999;37(5):437-445.
20. Kontio J. Software engineering risk management: a method, improvement framework, and empirical evaluation. Doctoral Dissertation (2001)
21. Roy GG. A risk management framework for software engineering practice, 2004 Australian software engineering conference. *Proceedings*, 2004, pp. 2004;60-67.
22. Risk management framework, SEI, Christopher J. Alberts and Audrey J. Dorofee. TECHNICAL REPORT. CMU/SEI-2010-TR-017. ESC-TR-2010-017 (2010)
23. Buglione L, Abran A, von Wangenheim CG, McCaffery F, Hauck JCR. Risk management: achieving higher maturity & capability levels through the LEGO approach. In *Software Measurement and the International Conference on Software Process and Product Measurement (IWSM-MENSURA), 2016 Joint Conference of the International Workshop on* (pp. 131-138). IEEE (2016)
24. *ISO/IEC 15504-5. Information Technology—Process Assessment—An Exemplar Software Life Cycle Process Assessment Model*. Geneva: International Organization for Standardization; 2012.
25. Proença D, Estevens J, Vieira R, Borbinha J. Risk management: a maturity model based on ISO 31000. In Business Informatics (CBI), 2017 IEEE 19th Conference on (Vol. 1, pp. 99-108). IEEE (2017)
26. Javaid MI, Iqbal M MW. A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). In Communication Technologies (ComTech), 2017 International Conference on (pp. 78-90), IEEE (2017)
27. Varajão J, Colomo-Palacios R, Silva H. ISO 21500: 2012 and PMBoK 5 processes in information systems project management. *Computer Standards & Interfaces*. 2017;50:216-222.
28. Öbrand L, Holmström J, Newman M. Navigating Rumsfeld's quadrants: a performative perspective on IT risk management. *Technology in Society*. 2017.
29. Pries-Heje J, Johansen J. Spi manifesto. *European System & Software Process Improvement and Innovation*. 2010.
30. *ISO/IEC/IEEE CD 16085: Systems and Software Engineering—Life Cycle Processes—Risk Management*. Geneva: International Organization for Standardization; 2018.
31. de Bruin T, Rosemann M, Freeze R, Kulkarni U. Understanding the main phases of developing a maturity assessment model. In: 16th Australasian conference on information systems (ACIS). Sydney (2005)
32. Becker J, Knackstedt R, Pöppelbuß J. Developing maturity models for IT management. *Business & Information Systems Engineering*. 2009;1(3):213-222.
33. Pöppelbuß J, Röglinger M. (2011). What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management. In ECIS (2011)
34. von Wangenheim G, Hauck JCR, Zoucas A, Salviano CF, McCaffery F, Shull F. Creating software process capability/maturity models. *IEEE Software*. 2010;27(4, July-Aug 2010):92-94.
35. Stallinger F, Plösch R. *Towards Methodological Support for the Engineering of Process Reference Models for Product Software. International Conference on Software Process Improvement and Capability Determination*. Springer International Publishing; 2014.
36. Renault A, Barafort B. "TIPA for ITIL—from genesis to maturity of SPICE applied to ITIL 2011", Proceedings of the 21th European System & Software Process Improvement and Innovation Conference 2014. Luxembourg (2014)
37. Di Renzo B et al. Operational risk management in financial institutions: process assessment in concordance with Basel II. *Software Process: Improvement and Practice*. 2007;12(4):321-330.
38. ISO Survey. http://www.iso.org/iso/iso-survey (online: accessed 20-May-2018) (2016)
39. Haufe K, Colomo-Palacios R, Dzombeta S, Brandis K, Stantchev V. A process framework for information security management. *International Journal of Information Systems and Project Management*. 2016;4(4):27-47.
40. *ISO/IEC 27013: TS Information Technology—Security Techniques—Guidance on the Integrated Implementation of ISO/IEC 27001 and ISO/IEC 20000-1*. Geneva: International Organization for Standardization; 2015.
41. *ISO/IEC 33072: TS Information Technology—Process Assessment—Process Capability Assessment Model for Information Security Management*. Geneva: International Organization for Standardization; 2016.
42. *ISO/IEC 33073: TS Information Technology—Process Assessment—Process Capability Assessment Model for Quality Management*. Geneva: International Organization for Standardization; 2017.
43. MacMahon ST, Cooper T, McCaffery F. Revising IEC 80001-1: risk management of health information technology systems. *Computer Standards & Interfaces*. 2018;60:67-72.
44. Pardo C, Pino FJ, García F, Piattini M, Baldassarre MT. An ontology for the harmonization of multiple standards and models. *Comput. Stand. Interfaces*. 2012;34(1):48-59. (2012)
45. *ISO Guide 73, Risk Management—Vocabulary*. Geneva: International Organization for Standardization; 2009.
46. *ISO/IEC DIS 20000-10: TS Information Technology—Service Management—Concepts and Terminology*. Geneva: International Organization for Standardization; 2018.
47. *ISO/IEC 27000: TS Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*. Geneva: International Organization for Standardization; 2016.

48. Barafort B, Mesquida AL, Mas A. Developing an integrated risk management process model for IT settings in an ISO multi-standards context. In International Conference on Software Process Improvement and Capability Determination (pp. 322-336). Springer, Cham (2017)

49. Barafort B, Mesquida AL, Mas A. Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context. *Computer Standards & Interfaces (to be published)* (2018)

50. Cortina S, Mayer N, Renault A, Barafort B. Towards a process assessment model for management system standards in: Proceedings of the International Conference SPICE 2014, Vilnius, Lithuania (2014)

How to cite this article: Barafort B, Mesquida A-L, Mas A. ISO 31000-based integrated risk management process assessment model for IT organizations. *J Softw Evol Proc*. 2019;31:e1984. https://doi.org/10.1002/smr.1984