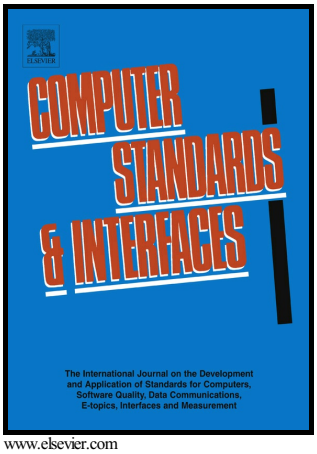
Integrating Risk Management in IT settings from ISO Standards and Management Systems Perspectives

Béatrix Barafort, Antoni-Lluís Mesquida, Antonia Mas



www.elsevier.com

PII: S0920-5489(16)30186-6
DOI: http://dx.doi.org/10.1016/j.csi.2016.11.010
Reference: CSI3172

To appear in: *Computer Standards & Interfaces*

Received date: 23 September 2016
Revised date: 21 November 2016
Accepted date: 24 November 2016

Cite this article as: Béatrix Barafort, Antoni-Lluís Mesquida and Antonia Mas Integrating Risk Management in IT settings from ISO Standards and Management Systems Perspectives, *Computer Standards & Interfaces* http://dx.doi.org/10.1016/j.csi.2016.11.010

Integrating Risk Management in IT settings from ISO Standards and Management Systems Perspectives

Béatrix Barafort[1], Antoni-Lluís Mesquida[2*] and Antonia 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, Ctra. de Valldemossa, km. 7.5, E07122 - Palma de Mallorca, Spain

beatrix.barafort@list.lu
antoni.mesquida@uib.es
antonia.mas@uib.es

[*]Contact information for the corresponding author. Dr. Antoni-Lluís Mesquida, Department of Mathematics and Computer Science, University of the Balearic Islands, Ctra. de Valldemossa, km. 7.5, E07122 - Palma de Mallorca, Spain

Abstract.

Organizational capabilities in companies, within IT settings, can be strengthened by a centralized and integrated risk management approach based on ISO standards. This paper analyses risk management activities throughout various selected ISO standards in order to provide the basis to improve, coordinate and interoperate risk management activities in IT settings for various purposes related to quality management, project management, IT service management and information security management. Taking as a basis the ISO 31000 international standard for risk management, a comparison is performed with the aim of identifying risk management related activities in the ISO high level structure for management system standards, ISO 9001, ISO 21500, ISO/IEC 20000-1 and ISO/IEC 27001. These standards are of high interest for practitioners in IT settings, benefitting from the integration of process-based activities, implementing mechanisms for linking IT and non-IT entities of their organization with risk management challenges to address. Integration vectors such as the understanding of the organisation and its context, risk-based thinking, leadership and commitment, process approach and PDCA structure are elicited.

Keywords: risk management, risk management process, integrated risk management, management system, integrated management system, IT settings, ISO standards.

1 Introduction

Information Technology is more than ever present, for business matters within companies, between interconnected companies and/or private individuals, for cloud computing solutions, Internet of Things, connected and mobile devices and many more Internet usages. IT has then become omnipresent and essential for any business. Because of its indispensable nature, risk management has also become vital. In all domains, risk management activities must be under control. It can be for dedicated risk management purposes or from a broader perspective in management systems (a management system is defined by ISO [1] as a "*set of interrelated or interacting elements of an organization ... to establish policies ... and objectives ... and processes ... to achieve those objectives";* Note 1 to this definition mentions that *"A management system can address a single discipline or several disciplines"*. In IT settings, many activities are strongly related to risk management: project management, information security and IT service management (ITSM) to quote the main domains. Risk is defined in [2] as "*effect of uncertainty on objectives*" and a Note to this definition mentions that "*Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process)"*.

Depending on their strategic goals, competitive advantage on the market, regulation and compliance constraints, IT companies or IT departments may need to be certified regarding management system standards such as the ISO/IEC 27001 [3] for information security or the ISO/IEC 20000-1 [4] for ITSM. They may also need to integrate these IT related standards with more general ones such as the ISO 9001 [5] for quality management system (QMS). This situation is more and more frequent and require integration and interoperability attentions for cost saving, complexity reduction, efficiency and effectiveness. This is particularly true for risk management which is central in IT organizations with integrated management systems and risk-based thinking.

In order to satisfy market constraints that many companies face today and to provide a broad and neutral perspective, the authors make the assumption that an integrated risk management approach for IT settings will benefit them by being based on ISO (International Organization for Standardization) standards. International standards represent international consensus, provide an open access to structured technical domains as well as voluntary positioning towards certifications, and contribute to companies' benefits. AFNOR, the French National Body for Standardization, has recently published a survey showing the benefits of standardization for the economy, with visible benefits on companies' results [6]. The ISO continuously promotes standardization benefits [7] and management system standards [8]. Every year, ISO performs a survey [9] of certifications to MSSs. The 2015 results show again that ISO 9001 (which gives the requirements for quality management systems) is the leader of management system certification standards.

This survey also indicates an increase of the certifications related to ISO/IEC 27001, and more recently ISO 22301 (Business continuity management systems). In 2015, ISO added a "new" management system standard: ISO/IEC 20000-1:2011 (Service management system requirements), after recommendations from international accreditation and certification experts that are consulted annually. Despite the fact that ITIL (IT Infrastructure Library) [10] remains the de facto standard in ITSM, ISO/IEC 20000-1 remains of interest for its alignment in intent and structure as a management system, for being closely related to ITIL processes, and a relative impact on the market [11]. Regarding Project management, we can quote that ISO 21500 (Guidance on Project management [12]) provides a globally accepted guideline in Project management. It identifies recommended generic project management processes. Even if they do not depict a management system targeting certification, process groups of ISO 21500 are based on the Plan-Do-Check-Act cycle for continuous improvement. The next evolutions could lead to an update transforming guidance into requirements and succeeding in a certification standard. So in intent and with a process-based approach, ISO 21500, ISO/IEC 27001 and ISO/IEC 20000-1 are closely related to the famous ISO 9001 standard for Quality management systems. These four ISO standards are of high interest for many practitioners in IT settings, interested by the integration of process-based activities, implementing mechanisms for making the link between IT and non-IT entities of their organization with Risk management challenges to address.

The objective of this research is to investigate and compare risk management activities throughout various selected ISO standards and to show that a centralized and integrated process-based risk management approach can provide the basis to improve, coordinate and interoperate risk management activities in IT settings for various purposes such as project management, quality management, ITSM, and information security management. By IT settings, we mean IT companies and IT departments, covering both development and operations sides, with projects and non-projects based activities. For the IT projects perspectives, we mean all kinds of IT projects including software engineering projects, IT infrastructure deployments... Considering the previous developments of this introduction, the following standards have been selected: ISO 9001, ISO 21500, ISO/IEC 27001 and ISO/IEC 20000-1. Finally, the structured input for these works is the international recognised normative reference in terms of Risk management: the ISO 31000 standard [13].Hence, the research question studied in this paper is: *how to integrate risk management in IT settings with a process-based approach within a management system context and benefit from selected ISO standards?* It is important to quote that this is a first stage of a bigger research aiming at looking for synergies in Risk management processes from these ISO standards point of view and at proposing artefacts such as Risk management process models. This is considered from a generic perspective enabling process-based Risk management integration, interoperability and improvement in IT settings with a management system environment. The results could be useful for the main varieties of IT organizations. Some specialisations to particular domains are not considered for now.

The paper is organized as follows: section 2 describes related work; section 3 is an overview of the studied standards; section 4 proposes the comparison approach and

the comparison itself; section 5 discusses and analyses the findings; section 6 tackles comparison extensions and section 7 concludes the paper.

2 Related Work

Integrating risk management has been studied from various perspectives in the literature. Many works have tackled the topic from close concepts points of view: harmonization and integration. In the Cambridge dictionary, harmonization is defined as follows: "*the act of making systems or laws the same or similar in different companies, countries, etc. so that they can work together more easily*". And integration is defined as: "*the process of combining two or more things into one*."

In the standardisation community, harmonization issues are a very big concern. An initiative in the Software and Systems sub-committee 7 in ISO/IEC JTC1 is aiming at proposing ontology to unify ISO software engineering standards [14]. Many concepts are tackled, and a metamodel for the management of goals, risks, and evidences provides an interesting insight on how concepts can be connected [15]. Harmonizing software development processes is also an important concern and mappings between processes and project settings have been investigated from the situational factors angle [16]. For the last years, more and more multi-frameworks analysis have been needed and performed by practitioners and researchers, for improvement or compliance purposes: optimisation of assessments in an industrial context have been tackled [17] as well as for the ISO/IEC 29110 with the ITMark certification schema assessing software processes of software companies [18].

More generally, harmonizing approaches have been proposed for quality frameworks and standards addressing Software Process Improvement practices; we can quote research works with case studies where ISO 9001 and CMMI-DEV have been harmonized and supported [19]. Pardo et al. have shown the complexity of using multiple standards and models and they propose a harmonization environment to address the issues with a process and a set of methods with an ontology [20] supporting the conceptual elements, and a web tool supporting the overall framework. A set of standards and models have been considered with case studies with the following models which can be relevant in IT settings: ISO 9001, CMMI, ISO/IEC 12207 and ISO/IEC 90003, ITIL, PMBOK and COBIT, ISO/IEC 27001, ISO/IEC 20000-1. This research team also proposes a process improvement approach based on multiple models [22].

From the integration perspective, integrating management systems has been a topic of interest in research and industry for many years now [23, 24]. This has been particularly true for quality management, environmental management and health and safety domains [9]. It has been more and more necessary to integrate these systems for cost reductions, efficiency, effectiveness, and market positioning.

In the IT domain, with the first publication in 2005 of the ISO/IEC 20000-1 and ISO/IEC 27001, new management system standards appeared on the international scene, respectively for ITSM and Information Security. Some integration models and approaches have been tackled [25, 26] with a model proposition for integrating

management systems [27], mainly driven by the ISO 9001 QMS implementation in a large number of companies.

In the meantime, maturity models, process assessment and improvement frameworks were very popular, such as CMMI [28] and ISO/IEC 15504 standards [29]. From a complementary perspective compared to a management system certification, performance management approaches dealing with process assessment and process improvement raised. An initiative in the medical device domain has also proposed a Risk Management Capability Model for the Medical Device Industry [30], based on Medical Device regulatory requirements and CMMI. Process Assessment Models (PAM), such as the PAM ISO/IEC 15504-8 [31], and the ISO/IEC 27001 Information Security one recently published by ISO [32], provide new methodological approaches for measurement and continual improvement, contributing to certification preparation and monitoring of the management system. Recently, a research contribution proposed a maturity model for an integrated management systems assessment [33]; it enables the comparison of integrated systems implemented in different companies or contexts.

As management system standards (MSS) interest increased, ISO published in its Directives in 2012 (revised in 2014) an annex named "High-level structure (HLS), identical core text, common terms and core definitions" for MSS [1]. The goal was to standardize the core content of management systems and to impose the adoption of this structure to all management systems to the rhythm of their respective revision. The ISO/IEC 27001 standard is from now on aligned with the HLS since its second revision in 2013 [3]. The ISO 9001 has been upgraded in its last revision of 2015 [5]. The ISO/IEC 20000-1:2011 [4] standard is partially aligned and still needs to be fully aligned with the HLS.

With a management system integration mindset, some R&D works have defined different generic processes related to the core content requirements of the HLS in a Process Assessment Model, using a Transformation Process based on Goal-oriented requirements engineering techniques [34, 35]. These works have been proposed to ISO and were incorporated within PRMs and PAMs for Information Security [32] and potentially for ISO/IEC 20000-1 and ISO 9001.

Among the integrative aspects of management systems, risk management is a particular topic of great importance and interest for organizations. A lot of research works exist, targeting risk management with applications in many domains. Thus Risk management plays an important part and is omnipresent in management systems. From the ISO standards perspective, the ISO 31000 standard on Risk management [6] is the main reference, with a holistic view on risk management. Furthermore, in many domains there are dedicated risk management standards: i.e. for Information security, we can quote the ISO/IEC 27005 (Information security risk management) [36]. Several approaches target methodologies for implementing risk management; we can cite [37] for Risk management in ISO/IEC 27001; we can also mention specific risks such as cloud computing ones [38]. When related to methodologies, these researches target the "How to", and do not concentrate on the "What" which is addressed by processes and then not being prescriptive when seen from a generic perspective.

Last but not least, IT settings are commonly organized by projects, and have to face projects risks. From the ISO perspective, the ISO 21500 [12] standard provides guidance for project management: processes, continual improvement and risk

management are important tackled concerns. This standard has been considered from a PRM and PAM point of view by the authors [39, 40] where a process-oriented organization can benefit from this high value structure for process assessment and process improvement purposes.

In the context of the problematic of integrated management systems, risk management is a critical cornerstone which has not been addressed specifically from the IT organizations point of view with a management system and process-based perspective. Considering the gained experience by the authors from the various domains, this paper intends to explore risk management in IT settings from the angle of the following selected more relevant ISO standards: ISO 31000 as main theme, ISO Annex SL, ISO 9001, ISO 21500, ISO/IEC 20000-1, and ISO/IEC 27001. Other standards such as the ISO/IEC 12207 Software lifecycle processes [41] and ISO/IEC 15288 System lifecycle processes [42] are not considered as they are not directly targeting a PDCA neither a management system approach.

3 Overview of targeted ISO standards for comparing Risk management

As mentioned in the introduction, ISO performs every year a survey of certifications to MSSs [9]. For ISO 9001, there has been more than one million certificates in 2015, 27536 certificates for ISO/IEC 27001 (increase of 20% compared to 2014) and 2778 for ISO/IEC 20000-1 which is the very "new" last standard included in this survey. This section is presenting each of the selected standards for the study, starting with the ISO 31000 on Risk management, then the High level structure for management system standards, followed by ISO 9001. The Guidance on Project Management ISO 21500 is then presented before ending with both ISO/IEC 27001 and ISO-IEC 20000-1.

3.1 ISO 31000:2009 Risk management – Principles and guidelines

The ISO 31000 standard on risk management provides principles and generic guidelines on risk management. It has become a generic and recognized reference in terms of risk management. This standard is not for the purpose of certification and does not provide requirements (there are no "SHALL statements"). It can be used whether for IT or non-IT applications, in public, private, associations or group. It is not specific to any industry or sector. As quoted by ISO, *"ISO 31000:2009 can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets. It can be applied to any type of risk, whatever its nature, whether having positive or negative consequences... It is intended that ISO 31000:2009 be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards"*.

ISO 31000 is currently being revised. Several discussions are going on in the international community involved in its revision. There is a debate on terminology as the definition of Risk is not perceived equally in all countries [43]. In Great Britain, risk is more oriented towards opportunities. In France, it is very oriented on danger and prevention. In Germany, national regulations prevail on the ISO 31000 application (stakeholders are more concerned by prevention and security of products and believe there are enough constraints; general guidelines such as the ones in ISO 31000 do not bring them enough value). There is another debate on the opportunity to transform ISO 31000 in a management system standard. As previously mentioned, ISO 31000 is not a certifying standard. The proposal for introducing the HLS, common to all MSS, has been rejected. ISO 31000 will remain a principles standard, without certification as a target.

Nevertheless, ISO 31000 represents a generic standard for risk management. The international community involved in its revision acknowledges its importance and its positioning regarding its guidelines and federating purpose. It appears to be complementary compared to various standards applicable to any sector and company size, such as ISO 9001 and can enable easily the setting up of a management system, without being prescriptive. It is also interesting to quote that in France, a working group in AFNOR (French standardization body) is developing an operational guide for intermediary, small and medium sized enterprises because of the need to help companies in understanding and deriving ISO 31000 to their context, whatever risk they encounter [44].

In this context, regarding our research objectives, ISO 31000 is the appropriate standard candidate for driving the comparison of risk management from a generic perspective, in various ISO standards.

3.2 ISO Annex SL: High level structure for management system standards

As previously mentioned, the HLS goal is to standardize the core content of management systems with the same structure. So it can address any discipline on the same way as appearing in the ISO Annex SL: "*In the Identical text proposals, XXX = an MSS discipline specific qualifier (e.g. energy, road traffic safety, IT security, food safety, societal security, environment, quality) that needs to be inserted"*. To follow the HLS ensures consistency among various MSS and enable easier integration. A lot of companies are constrained to put in place several management systems for different domains (information security, service management, quality, etc...). Reducing costs and providing the transversal approach via processes can be fulfilled by integrated and interoperable management systems. The HLS provides generic requirements to fulfil: risks and opportunities are among them.

ISO Technical Management Board progressively enforces the use of this High Level Structure to all management system standards, and then naturally targets risk management on a consistent way. As quoted in the following paragraphs, ISO 9001 and ISO/IEC 27001 are already aligned with the HLS whereas ISO/IEC 20000-1 is currently under revision, notably for this objective.

3.3 ISO 9001:2015 Quality management systems - Requirements

The flagship standard ISO 9001 providing requirements for quality management systems (QMS) has been revised and published in September 2015. This new version of ISO 9001 is aligned with the changes that organizations have to face, focusing more on performance, combining the process approach with risk-based thinking and activating the Plan-Do-Check-Act cycle at all levels of the organization. This new version has been designed for making easier the integration of several management systems (alignment with HLS). Moreover, it tackles a risk-based approach: "*The concept of risk-based thinking has been implicit in previous editions of this International Standard including, for example, carrying out preventive action to eliminate potential nonconformities, analysing any nonconformities that do occur, and taking action to prevent recurrence that is appropriate for the effects of the nonconformity. To conform to the requirements of this International Standard, an organization needs to plan and implement actions to address risks and opportunities. Addressing both risks and opportunities establishes a basis for increasing the effectiveness of the quality management system, achieving improved results and preventing negative effects.*"

3.4 ISO 21500:2012 Guidance on project management

ISO 21500 provides guidance for project management and can be used by any type of organization, for any type of project, irrespective of complexity, size or duration. This international standard provides high-level description of concepts and processes that are considered to form good practice in project management. It identifies the recommended project management processes to be used during a project as a whole, for individual phases or both.

It is admitted than the PMBOK Guide® [45] had a great influence on the ISO 21500 standard development. In this context, as in PMBOK, risk management in one of the ten existing subject groups and has processes in planning, implementing and controlling phases of the project life cycle.

ISO 21500 is currently an informative standard, based on globally accepted good practices. In the future, according to potential market demands, it could become a normative standard with requirements and a certification thrown in. When ISO 21500 was developed, ISO 9001 and ISO 31000 were used as references.

3.5 ISO 20000-1:2011 IT Service Management - Service management system requirements

The ISO/IEC 20000-1 is a service management system (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS. The requirements include the design, transition, delivery and improvement of services to fulfil agreed service requirements.

As the HLS was released in 2012 by ISO, the current version of ISO/IEC 20000-1 is not fully aligned with the HLS but has many requirements related to risk management with a close mind-set.

The ISO/IEC 20000-1 is currently being revised in particular for aligning with the HLS. In the draft revised document, ISO 31000 is cited as a reference for generic risk management.

3.6 ISO 27001:2013 Information security management

The ISO/IEC 27001 is part of the ISO 27000 family of standards which is aiming at helping organizations keep information assets secure. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS). An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It can be applied to small, medium and large businesses in any sector.

It includes people, processes and IT systems by applying a risk management process. It is aligned with the HLS.

The information security risk assessment and treatment process in ISO/IEC 27001 aligns with the principles and generic guidelines provided in ISO 31000, as well as establishing the external and internal context of the organization.

4 Comparison of Risk management in targeted ISO standards

In order to compare risk management approaches in the various selected ISO standards previously mentioned, after studying and screening all targeted ISO standards, the following systematic method has been followed:

- Step 1: Identification of risk-based activities in all compared standards (search on the keyword “Risk”).
- Step 2: Mapping of the sections/requirements to some sections in Clause 4 (Framework) or 5 (Process) of ISO 31000.
- Step 3: Description of relations or connection points among risk-based activities and the related requirements.

Table 1 summarizes the results of steps 1 and 2. The following sub-sections present each step on a detailed way.4.1 Step 1 - Identification of risk-based activities in all standards

The keyword “Risk” has been searched in all standards and appears in all standards in more intensity in some parts than others:

Table 1. Summary of the comparison process.

	Sections/requirements of the Standard addressing “risks”	Sections mapped to some requirement in ISO 31000 clauses 4 or 5
Annex SL	1	1

ISO 9001	14	12
ISO 21500	17	17
ISO/IEC 20000-1	12	12
ISO/IEC 27001	9	7

4.2 Step 2 - Mapping of the sections/requirements to some sections in Clause 4 (Framework) and 5 (Process) of ISO 31000

Table 2 presents the performed mapping as detailed below. The comparison shows that many similarities exist for risk management in the selected standards. The context of risk management is displayed via the policies, leadership and commitment, and the risk management itself is shown throughout the PDCA cycle with a dedicated process or set of processes for risk management in all standards.

Table 2. Mapping of ISO 31000 with other selected standards.

ISO 31000:2009	ANNEX SL	ISO 9001:2015	ISO 21500:2012	ISO/IEC 20000-1:2011	ISO/IEC 27001:2013
4 FRAMEWORK					
4.1 General					
4.2 Mandate and commitment		5.1.1 General 5.1.2 Customer focus 9.3.2 Management review inputs		4.1.1 Management commitment	5.1 Leadership and commitment
4.3 Design of framework for managing risks					
4.3.1 Understanding of the organization and its context					
4.3.2 Establishing risk managementpolicy		0.3.3 Risk-based thinking 6.1 Actions to address risks and opportunities A.5 Applicability	3.4 Organizational strategy and projects 3.4.1 Organizational strategy 4.3.3 Develop project plans 4.3.12 Create work breakdown structure 4.3.25 Estimate costs 4.3.26 Develop budget	4.5.2 Plan the SMS (Plan) 5.2 Plan new or changed services 6.6.1 Information security policy	5.2 Policy 6.2. Information security objectives and plans to achieve them

4.3.3 Accountability					
4.3.4 Integration into organizational processes		0.3 Process approach 0.3.1 General 4.4 Quality management system and its processes (4.4.1) 6.1 Actions to address risks and opportunities	4.1 Project management process application 4.3.6 Control changes 4.3.23 Develop schedule	4.5.3 Implement and operate the SMS (Do) 6.6.2 Information security controls 9.1 Configuration management 9.2 Change management	4.4 Information security management system 6.1 Actions to address risks and opportunities
4.3.5 Resources			3.9 Competencies of project personnel		
4.3.6 Establishing internal communication and reporting mechanisms			3.6 Project Governance 4.3.40 Manage communications		
4.3.7 Establishing external communication and reporting mechanisms			4.3.40 Manage communications		
4.4 Implementing risk management					
4.4.1 Implementing the framework for managing risk					
4.4.2 Implementing the risk management process					
4.5 Monitoring and review of the framework		6.1 Actions to address risks and opportunities		4.5.4.3 Management review	6.1 Actions to address risks and opportunities
4.6 Continual improvement of the framework				4.5.5.2 Management of improvements	
5.2 Communica-tion and consultation		4.2 Understanding the needs and expectations of interested parties	4.3.40 Manage communications		4.2 Understanding the needs and expectations of interested parties
5.3 Establishing the context	4.1 Understanding the organization and its context	4.1 Understanding the organization and its context			

5.3.1 Establishing the internal context					
5.3.2 Establishing the external context		4.1 Understanding the organization and its context A.8 Control of externally provided processes, products and services	3.5.2 Factors outside the organizational boundary 3.11 Project constraints		4.1 Understanding the organization and its context
5.4 Risk assessment				6.3.1 Service continuity and availability requirements 6.6.1 Information security policy	6.1.2 Information security risk assessment 6.2. Information security objectives and plans to achieve them 8.2 Information security risk assessment (operation)
5.4.2 Risk identification	6.1 Actions to address risks and opportuni-ties	6.1 Actions to address risks and opportunities (6.1.1)	4.3.28 Identify risks	6.6.3 Information security changes and incidents.	6.1.2 Information security risk assessment (c)
5.4.3 Risk analysis		9.1.3 Analysis and evaluation	4.3.29 Assess risks		6.1.2 Information security risk assessment (d)
5.4.4 Risk evaluation		9.1.3 Analysis and evaluation	4.3.29 Assess risks		6.1.2 Information security risk assessment (e)
5.5 Risk treatment	6.1 Actions to address risks and opportuni-ties	6.1 Actions to address risks and opportunities (6.1.2)	4.3.30 Treat risks		6.1.3 Information security risk treatment 6.2. Information security objectives and plans to achieve them 8.3Information security risk treatment

5.5.3 Preparing and implementing risk treatment plans	6.1 Actions to address risks and opportuni-ties	6.1 Actions to address risks and opportunities		
		9.1.3 Analysis and evaluation		
5.6 Monitoring and review		9.3.2 Management review inputs 10.2 Nonconformity and corrective action	4.3.31 Control risks	9.3 Management review (e)

4.3 Step 3 - Description of relations or connection points among risk-based activities

The relations detected during Step 3 are presented in the rest of this section according to the following classification:

- Context of risk management in all standards (section 4.1 in ISO 31000)
- Leadership and commitment (section 4.2 in ISO 31000)
- Plan-Do-Check-Act (PDCA) cycle (section 4.3 in ISO 31000)

It should be noted that when no relation was found between a category and a standard, no reference to this standard is made in the section.

4.3.1 Context of Risk management in all standards

ISO 31000 recommends that organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture.

Risk-based thinking is explicit in ISO 9001: "*an organization needs to plan and implement actions to address risks and opportunities. Addressing both risks and opportunities establishes a basis for increasing the effectiveness of the quality management system, achieving improved results and preventing negative effects"* (0.3.3).

ISO/IEC 27001 includes *"Requirements for the assessment and treatment of information security risks tailored to the needs of the organization"* (1). Moreover, *"The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed"* (0.1).

4.3.2 Leadership and commitment

According to ISO 31000, the introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organization, as well as strategic and rigorous planning to achieve commitment at all levels.

ISO 9001 explicitly assigns some leadership responsibilities for risk management to Top management: *"Top management shall demonstrate leadership and commitment with respect to the quality management system by promoting the use of the process approach and risk-based thinking"* (5.1.1). *"Top management shall demonstrate leadership and commitment with respect to customer focus by ensuring that the risks and opportunities that can affect conformity of products and services and the ability to enhance customer satisfaction are determined and addressed"* (5.1.2).

ISO/IEC 20000-1 also considers that *"Top management shall provide evidence of its commitment to planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the SMS and services by ensuring that risks to services are assessed and managed"* (4.1.1).

4.3.3 Plan-Do-Check-Act (PDCA) cycle

Plan

According to ISO 31000, the risk management policy should clearly state the organization's objectives for, and commitment to, risk management.

ISO 9001 considers that *"Risk-based thinking is essential for achieving an effective quality management system"* (0.3.3) and recommends that *"The organization shall plan actions to address risks and opportunities; and how to integrate and implement these actions into its quality management system processes; and evaluate their effectiveness"* (6.1.2).

ISO 21500 considers risk management as part of the organizational strategy *"Opportunities selection includes consideration of various factors, such as how benefits can be realized and risks can be managed"* (3.4.1).

ISO/IEC 20000-1, when planning the SMS, proposes to take into consideration that *"the service management plan shall contain or include the approach to be taken for the management of risks and the criteria for accepting risks"* (4.5.2). Also, *"Planning for the new or changed services shall contain or include the identification, assessment and management of risks"* (5.2).

In the same way as in ISO 9001, when planning for the information security management system according to ISO/IEC 27001, we can find that *"The organization shall determine the risks and opportunities that need to be addressed"* (6.1.1). And that "*The information security objectives shall take into account risk assessment and risk treatment results*" (6.2).

According to ISO 31000, risk management should become part of those organizational processes and embedded in all the organization's practices and processes in a way that it is relevant, effective and efficient.

In order for a project following the ISO 21500 recommendations to be successful, *"The project scope within the constraints, while considering the project risks and resource needs to provide the project deliverables, should be defined and managed"* (4.1).

In ISO 9001, it can be read that *"The organization shall determine the processes needed for the quality management system and their application throughout the organization, and shall address the risks and opportunities"* (4.4.1).

The ISO/IEC 20000-1 Change management process (9.2) also consider the impact of risks in the organizational processes: *"Decision-making shall take into consideration the risks, the potential impacts to services and the customer, service requirements, business benefits, technical feasibility and financial impact"*.

Do

In ISO 31000, when implementing risk management, an organization should implement the framework for managing risk and should ensure that the risk management process is applied through a risk management plan at all relevant levels and functions of the organization. The risk management process is shown in Figure 1 and comprises the activities described in ISO 31000 clauses 5.2 to 5.6.

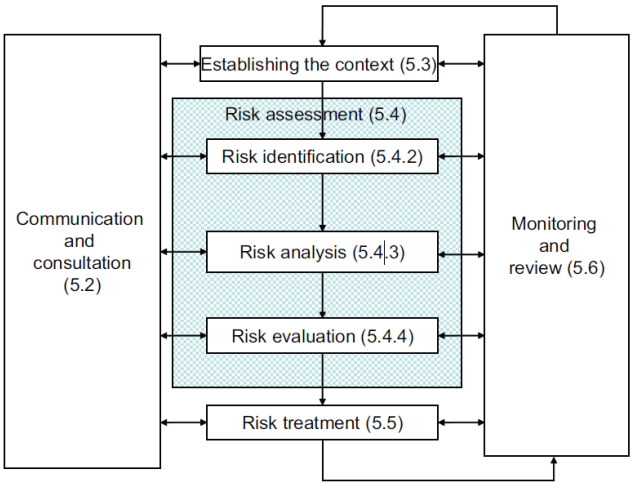


Fig. 1. ISO 31000 Risk management process

Communication and consultation (5.2) with external and internal stakeholders should take place during all stages of the risk management process.

ISO Annex SL defines a clause for understanding the needs and expectations of interested parties: *"The organization shall determine the interested parties that are relevant to the XXX management system; and the relevant requirements of these interested parties"* (4.2). ISO 9001 contains an instantiation of this clause to the

QMS: *"Due to their effect or potential effect on the organization's ability to consistently provide products and services… the organization shall determine the interested parties that are relevant to the quality management system; and the requirements of these interested parties that are relevant to the quality management system"* (4.2). The same clause can be found in ISO/IEC 27001 for the ISMS: *"The organization shall determine interested parties that are relevant to the information security management system; and the requirements of these interested parties relevant to information security"* (4.2).

ISO 21500 contains a specific process, Manage communications (4.3.40), which is focused on *"Resolving communication issues to minimize the risk that the project is negatively affected by unknown or unresolved stakeholder issues or misunderstandings"*.

By **establishing the context (5.3)**, the organization articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process.

ISO Annex SL defines a clause for understanding the organization and its context: *"The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its XXX management system"* (4.1). ISO 9001 and ISO/IEC 27001 contain instantiations of this clause for, respectively, a QMS and an ISMS.

ISO 21500 proposes to consider *"Factors outside the organizational boundary may have an impact on the project by imposing constraints or introducing risks affecting the project"* (3.5.2).

Risk assessment (5.4) is the overall process of risk identification, risk analysis and risk evaluation.

ISO/IEC 20000-1 states that *"The service provider shall assess and document the risks to availability and continuity of services. The agreed requirements shall take into consideration risks"* (6.3.1). In (6.6.1), this standard also suggests that "*Management with appropriate authority shall ensure that information security risk assessments are conducted at planned intervals"*.

Similarly, ISO/IEC 27001 considers that *"The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur. The organization shall retain documented information of the results of the information security risk assessments"* (8.2).

In **Risk identification (5.4.2)**, the organization should identify sources of risk, areas of impacts, events and their causes and their potential consequences.

ISO Annex SL defines a clause to *"…determine the risks and opportunities that need to be addressed*" (6.1). ISO 9001 contains an instantiation of this clause (6.1.1).

ISO 21500 contains a process named Identify risks whose purpose is "*To determine potential risk events and their characteristics that, if they occur, may have a positive or negative impact on the project objectives*" *(*4.3.28).

ISO/IEC 20000-1 considers that *"Requests for change shall be assessed to identify new or changed information security risks. Information security incidents shall be managed using the incident management procedures, with a priority appropriate to the information security risks*" (6.6.3).

ISO/IEC 27001 also contains a clause *"To identify the information security risks. To apply the information security risk assessment process to identify risks associated*

with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and to identify the risk owners" (6.1.2).

Risk analysis (5.4.3) involves developing an understanding of the risk. Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods.

ISO 21500 defines the Assess risks process (4.3.29) *"To measure and prioritize the risks for further action. This process includes estimating the probability of occurrence of each risk and the corresponding consequence for project objectives, if the risk does occur"*.

ISO/IEC 27001 explicitly considers "*analysing the information security risks. To assess the potential consequences that would result if the risks identified were to materialize; To assess the realistic likelihood of the occurrence of the risks identified and to determine the levels of risk*" (6.1.2).

The purpose of **risk evaluation (5.4.4)** is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation.

ISO/IEC 27001 states that information security risks should be evaluated *"By comparing the results of risk analysis with the risk criteria and prioritizing the analysed risks for risk treatment*" (6.1.2).

Risk treatment (5.5) involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls.

ISO Annex SL defines a clause to *"Plan actions to address these risks and opportunities"* (6.1). ISO 9001 contains an instantiation of this clause (6.1.2).

ISO 21500 Treat risks process (4.3.30) that *"Develops options and determines actions to enhance opportunities and reduce threats to project objectives. 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"*.

ISO/IEC 27001 proposes that *"The organization shall define and apply an information security risk treatment process"* (6.1.3). Moreover, *"The organization shall retain documented information of the results of the information security risk treatment"* (8.3).

Both **monitoring and review (5.6)** should be a planned part of the risk management process and involve regular checking or surveillance. It can be periodic or ad hoc.

ISO 9001 claims that *"The organization shall analyse and evaluate appropriate data and information arising from monitoring and measurement. The results of analysis shall be used to evaluate the effectiveness of actions taken to address risks and opportunities"* (9.1.3). And adds *"When a nonconformity occurs, including any arising from complaints, the organization shall update risks and opportunities determined during planning, if necessary"* (10.2.1).

ISO 21500 defines a process named Control risks (4.3.31), whose goals are *"Tracking the identified risks, identifying and analysing new risks, monitoring trigger conditions for contingency plans and reviewing progress on risk treatments while evaluating their effectiveness"*.

Check

According to ISO 31000, in order to ensure that risk management is effective the organization should measure risk management performance against indicators; periodically measure progress against the risk management plan and review the effectiveness of the risk management framework, policy and plan. These activities are proposed to be done during Management reviews in ISO 9001, ISO/IEC 20000-1 and ISO/IEC 27001.

ISO 9001 states that *"The management review shall be planned and carried out taking into consideration the effectiveness of actions taken to address risks and opportunities"* (9.3.2). In ISO/IEC 20000-1 *"Top management shall review the SMS and the services at planned intervals to ensure their continued suitability and effectiveness. This review shall include risks"* (4.5.4.3). Similarly, in ISO/IEC 27001 *"Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of results of risk assessment and status of risk treatment plan"* (9.3).

Act

According to ISO 31000, based on results of monitoring and reviews, decisions should be made on how the risk management framework, policy and plan can be improved.

Only ISO/IEC 20000-1 explicitly states that *"The service provider shall manage improvement activities including risk reduction"* (4.5.5.2). The rest of the analysed standards do not contain a sentence related to risk management improvement.

5 Analysis and findings

The comparison of Risk management in targeted ISO standards enabled to map the clauses of ISO 31000 regarding clauses of other standards and to show many common areas.

It is important to quote that all ISO management systems standards from now on inherit from the HLS a clause specifying the "*Understanding of the organization and its context*". This clause says: "*The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its XXX management system*". This clause has in fact been inherited itself from the ISO 31000. The external context of the organization has to be considered, with for instance regulatory and legal aspects, relationships with external stakeholders, etc. The internal context may include governance, capabilities including processes, information systems, etc.

Then we can say that the risk management context is highly connected to the management systems for ISO 9001, ISO/IEC 20000-1 and ISO/IEC 27001 and to the project environment in ISO 21500 with factors inside or outside the organizational

boundary. These factors may have an impact by introducing risks to the project; then risks should be managed explicitly.

According to ISO 9001, one of the key purposes of a management system is to act as a preventive tool. The concept of preventive action is expressed through the use of risk-based thinking. Top management should provide leadership and commitment for introducing risk-based thinking at the needed levels in the organization. Each organization decides the degree of formalism for addressing risk management and is responsible for the application of risk-based thinking. This provides a great flexibility which has to be balanced with the fact to address several disciplines and risk areas (quality, project, IT services, and information security) with integrated management systems.

Process approach and PDCA structure used in ISO 9001, ISO/IEC 20000-1 and ISO/IEC 27001 facilitate the integration of the different specific activities for planning risk management, performing risk treatment plans, monitoring if risk management process is effective, and improving the applied risk management framework. ISO 21500 uses a similar structure at the level of a particular project by suggesting actions to identify risks, apply mitigation and contingency actions, monitor if risk treatment plan is effective, and improve the project risk management activities.

In management systems and in projects, the process approach can drive the transversal mechanisms in order to better perform risk management activities. The 2015 version of ISO 9001 supports the idea of a risk management process for federating activities (even if it is not prescriptive). From the project management perspective, the fact to establish a risk management process can enforce the influence of risk management in organizations. The intensity and the types of risks are important in the ISO/IEC 27001: even if an integrated approach of risk management related to the management system can be put in place, a dedicated instance may be implemented for the information security context which is very specific and critical. ISO/IEC 20000-1 may soon follow the same idea by fully aligning to the HLS. Again, each set of risks related to some dedicated scope (quality, project, IT service, information security) can be managed from a dedicated implementation derived from a unique generic risk management process.

6 Extending the comparison

The analysis described in Section 5 shows the strong similarities that can be found in the studied standards and that are vectors for integration: HLS and management system, process approach, common terms for risks and similar structures for managing risks (with risk assessment composed of risk identification, risk analysis and risk evaluation, and risk treatment). To further compare the selected standards of our work, we aim at identifying groups of statements with common meanings and goals, with three criteria to respect: integration, interoperability and completeness. That could lead to the identification of processes, processes being major integrating and interoperability vectors, in particular in a management system context. With this process-thinking objective, the Transformation process [34] can be applied and be

extended to multiple standards as inputs. So it can take into account the multi-frameworks coverage of our approach with various sources of information as inputs.

In our work, the information is coming from guidelines or guidance standards (ISO 31000 as the main standard and ISO 21500) with recommendations ("SHOULD" statements), permissions ("MAY" statements) and possibility and capability ("CAN" statements), as quoted in the ISO Directives Part 2 for drafting international standards (Clause 7: Verbal forms for expressions of provisions) [46]. The information is also coming from requirements standards ("SHALL" statements) such as ISO/IEC 20000-1, ISO/IEC 27001 and the Annex SL of ISO Directives Part 1.

So as to analyse systematically our main generic reference on Risk management, elementary statements have been determined from all statements (as if it was a collection of requirements/information as stated in [34]) of clauses 4 and 5 in ISO 31000. 283 elementary statements have been found (Table 3). The text has been analysed in ISO 31000 in order to help determining the main sets of statements.

Table 3. ISO 31000 text analysis for clauses 4 and 5.

	Number of occurrences
Information statement	44
SHOULD statement	161
CAN statement	57
MAY statement	21

According to this analysis, the "SHOULD" statements are considered as the most important activities candidates for some common activities. Each elementary statement can be grouped according to the comparison explained in Section 5, and by organising and structuring the information by topics from clauses. We can quote for instance Mandate and Commitment, Establishing risk management policy, Communication and consultation, Defining risk criteria, Risk identification, etc.

Some previous research works can also be exploited [35] as well as the recent published ISO standard with a process assessment model based on the ISO/IEC 27001 [32] so that common processes for management system standards provide some inputs on groupings. In [32], the following processes are proposed as common processes for management systems: Communication management, Documentation management, Human resource management, Improvement, Internal audit, Management review, Non-conformity management, Operational planning, Operational implementation and control, Performance evaluation, Risk and opportunity management. These common processes can influence the groupings, for instance on aspects such as Communication, Improvement, and Review. But a targeted granularity has to be kept in mind for addressing Risk management on the best way. Indeed the overall Risk management process tackled in Clause 5 of ISO 31000 can lead to a detailed breaking down of activities such as the followings: risk identification, risk analysis, risk evaluation and risk treatment seen separately (ISO 21500 provides the same detailed approach with Identify risks, Assess risks, Treat risks, and Control risks), or to a more compacted view with an overall risk assessment (comprising risk identification, risk analysis, risk evaluation) and risk treatment "only". From a macroscopic view on Risk management, management system standards propose a unique "Risk and opportunity

management" set of statements. This can be extended with the ISO 31000 being generic but providing a more detailed view on Risk management process.

Processes and PDCA method foster interoperability with a systemic approach: the activities of the processes throughout their inputs and outputs are inter-operating. Driven by the ISO 31000 elementary statements determination, all other selected standards will also have to be analysed systematically (focus on "SHOULD" statements for ISO 21500, and on "SHALL" statements for other ISO targeted standards) and mapped compared with ISO 31000, with traceability to all statements (according to the Transformation process [34]). It will enable to get a complete picture and target integration objectives, with the foreseen research results from a process model perspective, as mentioned in the conclusion below.

7 Conclusion

In this paper we present a comparison of how risk management is tackled in several ISO standards (ISO 31000, HLS, ISO 9001, ISO 21500, ISO/IC 20000-1 and ISO/IEC 27001) that can be deployed in IT settings with management systems and how this comparison can be extended to further research works. This comparison contributes to the exploration of how Risk Management can be integrated in such contexts. Several facets of management system(s) are integration vectors such as the understanding of the organisation and its context, risk-based thinking, leadership and commitment, process approach and PDCA structure.

Considering the above-mentioned management system integration vectors, we believe that organizational capabilities in companies with IT settings can be strengthened by an integrated risk management process or set of processes, based on ISO standards such as the compared ones in this paper. The selected standards were voluntarily limited because there are empirically considered as the most significant in IT settings, as traced back by practitioners to the authors. An integrated risk management process or set of processes can be described on a very structured way enabling process assessment against a capability measurement framework and facilitating process improvement. In this context the authors intend to develop a process reference model and a process assessment model (satisfying requirements of the ISO/IEC 33004 standard [47]) dedicated to risk management, but aligned to various selected ISO standards, for providing a centralized and integrated risk management approach with improvement, coordination and interoperability characteristics. This enables process assessment and improvement where management, definition and deployment, measurement and continual improvement are dealt with. Thus it will allow integrating risk management in IT settings with a systemic management of quality, project, IT services and information security such as tackled by ISO standards related to these disciplines in the paper. Other ISO standards such as ISO/IEC 12207 and ISO/IEC 15288, and ISO/IEC 27005 may be considered, but the scope of the research question limited to ISO standards, a management system context and PDCA approach will remain the main drivers.

Our intention is to develop generic (for all IT organizations that meet our definition of IT setting) risk management process improvement models that could be, in the

future, adapted to the nature of specific IT settings in particular contexts. The results presented in this paper represent the first step towards the development of risk management process models, which will facilitate the assessment and improvement of risk management activities in IT settings. Various case studies will be performed in the future, thanks to the collaboration with IT settings in different sectors with diverse size, level of management system maturity and vision of risk management. The doors for integrated risk management with management systems of other domains than IT may also be opened as we already tackle the very popular ISO 9001 standard and the promising ISO 21500 one on Project management.

Acknowledgments. This work has been partially supported by the Spanish Ministry of Science and Technology with ERDF funds under grants TIN2016-76956-C3-3-R and TIN2013-46928-C3-2-R. Xxx LIST?

References

1. ISO/IEC Directives, Part1. Annex SL Proposals for management system standards. International Organization for Standardization, Geneva (2014)
2. ISO Guide 73, Risk management — Vocabulary. International Organization for Standardization, Geneva (2009)
3. ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization, Geneva (2013)
4. ISO/IEC 20000-1: Information Technology — Service management — Part 1: Service management system requirements. International Organization for Standardization, Geneva (2011)
5. ISO 9001: Quality management systems – Requirements. International Organization for Standardization, Geneva (2015)
6. Afnor normalisation, Standardization: a Genuine Advantage for the Economic Activity of Companies that get Involved in it, Association Française de Normalisation, Paris (2016)
7. http://www.iso.org/iso/home/standards/benefitsofstandards.htm
8. http://www.iso.org/iso/home/standards/management-standards.htm
9. ISO Survey (2015). http://www.iso.org/iso/iso-survey
10. The Cabinet Office. ITIL Lifecycle Publication Suite. The Stationery Office Edition (2011)
11. Cots, S., Casadesús, M.: Exploring the service management standard ISO 20000. Total Qual. Manage. Bus. Excellence 26(5-6), 515–533 (2015). Taylor Francis Online
12. ISO 21500: Guidance on project management. International Organization for Standardization, Geneva (2012)
13. ISO 31000: Risk management – Principles and guidelines. International Organization for Standardization, Geneva (2009)
14. Henderson-Sellers, B., Gonzalez-Perez, C., Mcbride, T., & Low, G. (2014). An ontology for ISO software engineering standards: 1) Creating the infrastructure. Computer Standards & Interfaces, 36(3), 563-576.

15. Larrucea, X., Gonzalez-Perez, C., McBride, T., & Henderson-Sellers, B. (2016). Standards-based metamodel for the management of goals, risks and evidences in critical systems development. Computer Standards & Interfaces, 48, 71-79.
16. Jeners, S., Clarke, P., O'Connor, R. V., Buglione, L., & Lepmets, M. (2013, June). Harmonizing software development processes with software development settings-a systematic approach. In European Conference on Software Process Improvement (pp. 167-178). Springer Berlin Heidelberg.
17. Larrucea, X., & Santamaria, I. (2014). An industrial assessment for a multimodel framework. Journal of Software: Evolution and Process, 26(9), 837-845.
18. Larrucea, X., Santamaría, I., & Colomo-Palacios, R. (2016). Assessing ISO/IEC29110 by means of ITMark: results from an experience factory. Journal of Software: Evolution and Process.
19. Baldassarre, M. T., Caivano, D., Pino, F. J., Piattini, M., & Visaggio, G. (2012). Harmonization of ISO/IEC 9001: 2000 and CMMI-DEV: from a theoretical comparison to a real case application. Software Quality Journal, 20(2), 309-335.
20. Pardo, C., Pino, F. J., García, F., Piattini, M., & Baldassarre, M. T. (2012). An ontology for the harmonization of multiple standards and models. Computer Standards & Interfaces, 34(1), 48-59.
21. Pardo, C., Pino, F. J., Garcia, F., Baldassarre, M. T., & Piattini, M. (2013). From chaos to the systematic harmonization of multiple reference models: A harmonization framework applied in two case studies. Journal of Systems and Software, 86(1), 125-143.
22. Pardo-Calvache, C. J., García-Rubio, F. O., Piattini-Velthuis, M. G., Pino-Correa, F. J., & Baldassarre, M. T. (2015). A 360-degree process improvement approach based on multiple models. *Revista Facultad de Ingeniería Universidad de Antioquia*, (77), 95-104..
23. Casadesús, M., Karapetrovic, S., Heras, I.: Synergies in standardized management systems: Some empirical evidence. TQM J. 23(1), 73–86 (2011). Emerald Insight
24. Simon, A., Karapetrovic, S., Casadesús, M.: Difficulties and benefits of integrated management systems. Ind. Manage. Data Syst. 112(5), 828–846 (2012). Emerald Insight
25. Mesquida, A.L., Mas, A.: Integrating IT service management requirements into the organizational management system. Comput. Stand. Interfaces 37, 80–91 (2015). Elsevier
26. Mesquida, A.L., Mas, A., Amengual, E., Cabestrero, I.: Sistema de gestión integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. Rev. Esp. Innovación Calidad e Ing. del Softw. 6(3), 25–34 (2010). ATI
27. Mesquida, A., Mas, A., San Feliu, T., Arcilla, M.: MIN-ITs: a framework for the integration of IT management standards in mature environments. Int. J. Software Eng. Knowl. Eng. 24(06), 887–908 (2014). World Scientific
28. CMMI for Development, Acquisition & Services, version 1.3. Carnegie Mellon University, Software Engineering Institute (2010)
29. ISO/IEC 15504-2: Information Technology — Process assessment — Performing an assessment. International Organization for Standardization, Geneva (2003)
30. Mc Caffery, F., Burton, J., Richardson, I.: Risk management capability model for the development of medical device software. Software Qual J (2010) 18: 81. doi:10.1007/s11219-009-9086-7
31. ISO/IEC TS 15504-8: Information Technology — Process assessment — An exemplar process assessment model for IT service management. International Organization for Standardization, Geneva (2012)

32. ISO/IEC 33072: TS Information Technology — Process Assessment — Process capability assessment model for information security management. International Organization for Standardization, Geneva (2016)
33. Domingues, P., Sampaio, P., Arezes, P.M.: Integrated management systems assessment: a maturity model proposal. J. Cleaner Prod. (2016). doi:10.1016/j.jclepro.2016.02.103
34. 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. Dorling, A., Rout, T., Treffny, R. (eds.) SPICE 2008. Global Association for Software Quality, Nuremberg (2008)
35. Cortina, S., Mayer, N., Renault, A., Barafort, B.: Towards a process assessment model for management system standards. In: Mitasiunas, A., Rout, T., O'Connor, R.V., Dorling, A. (eds.) SPICE 2014. CCIS, vol. 477, pp. 36–47. Springer, Heidelberg (2014)
36. ISO/IEC 27005: Information technology– Security techniques – Information security risk management – Requirements. International Organization for Standardization, Geneva (2011)
37. Parra, A. S. O., Crespo, L. E. S., Alvarez, E., Huerta, M., & Paton, E. F. M. (2016). Methodology for Dynamic Analysis and Risk Management on ISO27001. IEEE Latin America Transactions, 14(6), 2897-2911.
38. Chou, D. C. (2015). Cloud computing risk and audit issues. Computer Standards & Interfaces, 42, 137-142.
39. Mesquida, A.-L., Mas, A., Lepmets, M., Renault, A.: Development of the project management SPICE (PMSPICE) framework. In: Mitasiunas, A., Rout, T., O'Connor, R.V., Dorling, A.(eds.) SPICE 2014. CCIS, vol. 477, pp. 60–71. Springer, Heidelberg (2014)
40. Mesquida, A.-L., Mas, A., Barafort, B.: The project management SPICE (PMSPICE) process reference model: towards a process assessment model. In: O'Connor, R.V., et al. (eds.) EuroSPI 2015. CCIS, vol. 543, pp. 193–205. Springer, Heidelberg (2015). doi:10.1007/978-3-319-24647-5_16
41. ISO/IEC 12207: Information technology – System and software engineering - Software lifecycle processes. International Organization for Standardization, Geneva (2008)
42. ISO/IEC/IEEE 15288: Information technology – System and software engineering - System lifecycle processes. International Organization for Standardization, Geneva (2015)
43. Enjeux – Le Magazine de la Normalisation et du Management. Association Française de Normalisation, Supplément N° 362, Paris (2016)
44. FD X 50-260: Management des risques – Lignes directrices pour la mise en œuvre dans les ETI/PME et autres organismes - ETI/PME-PMI. Association Française de Normalisation, Paris (2016)
45. Guide A. Project Management Body of Knowledge (PMBOK® GUIDE). Project Management Institute (2001)
46. ISO/IEC Directives Part 2. Principles and rules for the drafting of ISO and IEC documents. International Organization for Standardization, Geneva (2016)
47. ISO/IEC 33004: Information Technology - Process assessment - Requirements for process reference, process assessment and maturity models. International Organization for Standardization, Geneva (2015)

Highlights

- Risk management in IT settings can be centralized and integrated from several ISO standards.
- Based on ISO 31000, risk management related activities in other standards are identified and compared.
- The comparison is performed with the ISO structure for management system standards, ISO 9001, ISO 21500, ISO/IEC 20000-1 and ISO/IEC 27001.
- The results are the first step towards the development of a process model for integrating risk management activities.