



Universitat
de les Illes Balears

DOCTORAL THESIS
2018

**Doctoral Programme of Information and
Communications Technology**

**INTEGRATED RISK MANAGEMENT
PROCESS IMPROVEMENT FRAMEWORK
IN IT SETTINGS BASED ON ISO STANDARDS**

Béatrix Barafort

Thesis Supervisor: Antònia Mas Pichaco
Thesis Supervisor: Antoni Lluís Mesquida Calafat

Doctor by the Universitat de les Illes Balears

Antònia Mas Pichaco, professora del Departament de Matemàtiques i Informàtica de la Universitat de les Illes Balears

FA CONSTAR:

que la present memòria "Integrated risk management process improvement framework in IT settings based on ISO standards" presentada per B atrix Barafort per optar al grau de Doctor en Tecnologies de la Informaci  i les Comunicacions, ha estat realitzada sota la seva direcci  i compleix els requisits per ser considerada com a tesi doctoral.

Firma i data

Antoni Llu s Mesquida Calafat, professor del Departament de Matem tiques i Inform tica de la Universitat de les Illes Balears

FA CONSTAR:

que la present mem ria "Integrated risk management process improvement framework in IT settings based on ISO standards" presentada per B atrix Barafort per optar al grau de Doctor en Tecnologies de la Informaci  i les Comunicacions, ha estat realitzada sota la seva direcci  i compleix els requisits per ser considerada com a tesi doctoral.

Firma i data

I dedicate this thesis to Mathis and Arthur, my dear sons.

Acknowledgements

I would first like to express my very deep gratitude to my thesis supervisors Professor Antònia Mas Pichaco and Dr. Antoni Lluís Mesquida Calafat for making this thesis happen in my particular context, advising and supporting me all along the works. I also thank all Spanish members of the research project in which this PhD thesis took place.

Deserving of my special thanks are my close colleagues of the Luxembourg Institute of Science and Technology (LIST) who supported me, contributed to the TIPA Framework and to the standardization journey: Stéphane Cortina, Michel Picard, Alain Renault, Samuel Renault and Philippe Valoggia, as well as Wided Guédria and Anne Hendrick. It has been and continue to be, a pleasure working with all of them. I thank all other colleagues in LIST who supported me in any way.

I would also like to express my gratitude to the management of the Luxembourg Institute of Science and Technology (LIST) who encouraged me for accomplishing this PhD thesis.

Finally, I would like to thank my wonderful sons Arthur and Mathis, who are my ray of sunshine in all moments, my brother, confidant and supporter, my mother who enabled me to become what I am today. And I have special thoughts for my late dear father and sister.

Funding

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

List of Manuscripts

As a compendium of articles, the content of this thesis consist of the following manuscripts which contributed to the State-of-the-Art (Chapter 2), to the Research approach (Chapter 3), and the main manuscripts (see C1, C2, C3 below) which constitute the full Research contribution (Chapter 4):

- C1. Barafort, B.; Mesquida, A.L. & Mas, A. **Integrating risk management in IT settings from ISO standards and management systems perspectives**. *Computer Standards & Interfaces*, Volume 54, Part 3, November 2017, Pages 176-185.
DOI: 10.1016/j.csi.2016.11.010

Impact factor:

- 1.465; Q2; 47/104 (Computer Science, Software Engineering)
InCites Journal Citation Reports 2017
- 0.378, Q2 (Computer Science, Software)
SCImago Journal Rank (SJR)

- C2. Barafort, B.; Mesquida, A.L. & Mas, A. **Integrated Risk Management Process Assessment Model for IT Organizations based on ISO 31000 in an ISO Multi-Standards Context**. *Computer Standards & Interfaces*, In Press, Corrected Proof, 2018.
DOI: 10.1016/j.csi.2018.04.010

Impact factor (in 2017):

- 1.465; Q2; 47/104 (Computer Science, Software Engineering)
InCites Journal Citation Reports 2017
- 0.378, Q2 (Computer Science, Software)
SCImago Journal Rank (SJR)

- C3. Barafort, B.; Mesquida, A.L. & Mas, A. **ISO 31000-based Integrated Risk Management Process Assessment Model for IT Organizations**. *Journal of Software: Evolution and Process* .To be published, 2018.
DOI: 10.1002/smr.1984

Impact factor (in 2017):

- 1.167; Q3; 58/104 (Computer Science, Software Engineering)
InCites Journal Citation Reports 2017
- 0.233, Q3 (Computer Science, Software)
SCImago Journal Rank (SJR)

- C4. Barafort, B.; Mesquida, A.L. & Mas, A. **How to Integrate Risk Management in IT settings within Management Systems? Comparison and Integration Perspectives from ISO Standards**. In *International Conference on Software Process Improvement and Capability Determination*, pp. 254-269. Springer, Cham (2016)
DOI: 10.1007/978-3-319-38980-6_19
Conference Ranking 2016: A

- C5. S. Cortina, B. Barafort, M. Picard, A. Renault, **Using a Process Assessment Model to prepare for an ISO/IEC 20000-1 Certification: ISO/IEC 15504-8 or TIPA for ITIL?**, In European Conference on Software Process Improvement (pp. 83-93). Springer, Cham (2016)
DOI: 10.1007/978-3-319-44817-6_7
Conference Ranking 2016: B
- C6. M. Picard, A. Renault, B. Barafort, S. Cortina, **Measuring Readiness for Compliance: a Gap Analysis tool to complete the TIPA Process Assessment Framework**, In European Conference on Software Process Improvement (pp. 106-116). Springer, Cham (2016)
DOI: 10.1007/978-3-319-44817-6_9
Conference Ranking 2016: B
- C7. Barafort, B., Mesquida, A. L., & Mas, A. **How to Elicit Processes for an ISO-Based Integrated Risk Management Process Reference Model in IT Settings?** In European Conference on Software Process Improvement (pp. 43-57). Springer, Cham (2017)
DOI: 10.1007/978-3-319-64218-5_4
Conference Ranking 2017: B
- C8. Lourinho, R., Almeida, R., da Silva, M. M., Pinto, P., & Barafort, B. **Mapping of Enterprise Governance of IT Practices Metamodels**. In European, Mediterranean, and Middle Eastern Conference on Information Systems (pp. 492-505). Springer, Cham (2017)
DOI: 10.1007/978-3-319-65930-5_39
Conference Ranking 2017: B
- C9. Barafort, B., Mesquida, A. L., & 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)
DOI: 10.1007/978-3-319-67383-7_24
Conference Ranking 2017: A
- C10. Cortina, S., Valoggia, P., Renault A. & Barafort, B. **Process Risk Determination supporting Data Protection Impact Assessment**. To be published in International Conference on Software Process Improvement and Capability Determination Springer, Cham (2018)

Table of Contents

1.	Introduction	1
1.1	History and background	1
1.1.1	The TIPA® Framework	1
1.1.2	Standardization background	3
1.2	Motivation of work	4
1.3	Research objectives	6
1.4	Research contributions	7
2.	State-of-the-Art	11
2.1	Integration perspectives	11
2.1.1	Harmonization in Software Engineering and Software Process Improvement	11
2.1.2	Integrating management system standards	12
2.1.3	Integrated risk management in literature	13
2.1.4	Risk management in IT and software contexts	14
2.1.5	Process models, process assessment and process improvement.....	15
2.2	Overview of ISO standards	16
2.2.1	ISO 31000:2018 Risk management – Principles and guidelines	16
2.2.2	ISO/IEC Directives Part 1 and Consolidated ISO Supplement – 2018 (9 th edition) - Annex SL: Proposals for Management System Standards – Appendix 2: High level structure.....	17
2.2.3	ISO 9001:2015 Quality management systems - Requirements	18
2.2.4	ISO 21500:2012 Guidance on project management	18
2.2.5	ISO/IEC 20000-1:2018 Part 1: Service management system requirements	19
2.2.6	ISO/IEC 27001:2013 Information security management systems - Requirements.....	19
2.2.7	ISO 22301:2013 Societal security - Business continuity management systems – Requirements	19

2.2.8	ISO/IEC 90006:2013 Guidelines for the application of ISO 9001:2008 to IT service management and its integration with ISO/IEC 20000-1:2011	20
2.2.9	ISO/IEC/IEEE 12207:2017 Systems and software engineering – Software life cycle processes	20
2.2.10	ISO/IEC/IEEE 15288:2015 Systems and software engineering – System life cycle processes	20
2.3	Study of relevant standards with Risk management process(es) in PAMs	21
2.4	ISO standards terminology for risk management.....	24
3.	Research approach according to Design Science	29
3.1	Problem identification and motivation.....	30
3.2	Definition of the objectives for a solution	30
3.3	Design and development	31
3.4	Demonstration.....	32
3.5	Evaluation.....	32
3.6	Communication	34
4.	Research Contributions.....	37
4.1	Research contribution C1.....	38
4.1.1	Abstract	38
4.1.2	C1 Paper.....	38
4.2	Research contribution C2.....	49
4.2.1	Abstract	49
4.2.2	C2 Paper.....	49
4.3	Research contribution C3.....	60
4.3.1	Abstract	60
4.3.2	C3 Paper.....	60
5.	Discussion and conclusion.....	77
5.1	Discussion.....	77

5.1.1	Investigation and comparison of risk management activities throughout selected ISO standards targeting management systems.....	77
5.1.2	Showing that a centralized and management systems approach based on processes contributes to integration in a process-centric risk management mindset.....	78
5.1.3	Proposal of means to improve risk management processes in IT settings.....	80
5.2	Conclusion and future works.....	82
5.2.1	Conclusion.....	82
5.2.2	Future works	82
6.	Annex - Terminology tables.....	85
7.	Annex – Elementary statements from ISO 31000:2018.....	93
8.	Annex - Requirement trees and goal trees for risk management specific processes.....	109
8.1	Requirement tree and goal tree for Risk criteria definition process	109
8.2	Requirement tree and goal tree for Risk identification process	110
8.3	Requirement tree and goal tree for Risk analysis process.....	112
8.4	Requirement tree and goal tree for Risk evaluation process.....	114
8.5	Requirement tree and goal tree for Risk treatment process	116
9.	Annex - IRMIS PAM	119
9.1	Introduction.....	119
9.1.1	Definition of a Process Assessment Model.....	119
9.1.2	Foreword	119
9.2	PAM process map	120
9.3	Description of processes	121
9.3.1	Top Management Process	121
9.3.2	Common Processes	123
9.3.3	Risk Management Processes.....	135
9.4	Process capability indicators for level 1 to 5.....	144

10. References..... 145

Abstract

Nowadays risk management is pervasive, concerns any sector in industry, and any discipline such as quality management, project management, service management and information security management. As in any type of organization, risk management omnipresence is very true in IT companies with the growing complexity of applications, devices, and interconnected networks. Market is demanding more and more certifications for companies to demonstrate how they can satisfy their customers, including an efficient and effective risk management approach. The International Organization for Standardization (ISO) proposes management system standards (MSSs), with the most popular one: ISO 9001, and in the IT domain ISO/IEC 20000-1 for IT service management system and ISO/IEC 27001 for information security management system. With also a process-based approach and risk-based thinking, the ISO 21500 standard tackles project management. These four ISO standards are of high interest for many practitioners in IT settings, concerned 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. IT settings mean IT companies and IT departments, covering both development and operations sides, with project and non-project based activities.

In order to improve and integrate risk management in IT settings with ISO standards as the basis representing international consensus of practices, the following main research question is targeted: *“How to improve risk management processes in IT settings from an integrated and management system perspective in multiple ISO standards?”*. Previous studies have reported integration perspectives at the ISO level and within best practices frameworks with harmonization effort on the concepts of these multiple frameworks (including risk management aspects), mainly in the software engineering and the software process improvement communities. It is more a topic of interest for integrating management systems, in particular with quality management, environmental management and health and safety domains for cost reductions, efficiency, effectiveness, and market positioning reasons. In literature, diverse frameworks and approaches to support integrated risk management have been developed, but none of them proposes a unified path. In the IT domain, software engineering plays a significant part but risk management is not addressed from a specific way. From a process performance perspective, several initiatives have proposed capability and maturity models (C&MM), with quite heterogeneous approaches. In this context, this research intends to explore risk management in IT settings from the angle of the following ISO standards: ISO 31000, the international reference in risk management, ISO Annex SL (high level structure for MSSs), ISO 9001, ISO 21500, ISO/IEC 20000-1 and ISO/IEC 27001 (as well as ISO/IEC 27005 on information security risk management for complementary inputs). Relevant standards with risk management processes in process assessment models have been studied, as they propose a risk management process description. Among these various processes, the risk management process, as addressed in the ISO 31000 standard, is very general. There is little difference between these processes generally describing a single risk management process, without detailed descriptions for various aspects of risk management (risk assessment as the overall process of risk identification, risk analysis and risk evaluation, and risk treatment). Some closely related works have been performed in the medical IT networks domain, but in the first place, they did not address the management system perspective; in

order to facilitate risk management process improvement, they finally adopted the same approach as this research work. For being up to date, a constant alignment with the latest version of each selected standard was performed during this PhD research, as well as a selection of the most appropriate risk management terminology over ISO standards.

This research is based on Design Science principles for creating artefacts in IT settings. A set of six activities was followed for creating a process reference model (PRM) and a process assessment model (PAM) for integrated risk management processes in IT settings (IRMIS) based on ISO standards, with iterations and interactions for improving the proposed solution related to the problem to be solved. First, in terms of problem identification and motivation, practitioners face manifold problems in industry regarding risk management improvement in the context of ISO standards in IT settings. For defining the objectives of the solution, ISO standards provide the material with requirements and guidance for defining a PRM and a PAM as well as expert knowledge in risk management. For designing and developing the artefacts, a nine-steps validated Transformation process is applied as a systematic approach. For demonstrating the problem solving, a first loop of validation has been performed with process, project and risk management experts; then evaluation of the IRMIS PRM and PAM has been performed with an evaluation grid supplemented by the analysis of each process, whether via reusing existing process descriptions from ISO committees or via the analysis of scientific experts via publication peer reviews. Finally, communication comprises scientific and professional events with publications, and a particular attention paid to the ISO community with the promotion of the IRMIS PRM and PAM in dedicated technical committees.

The research contribution consists in three main lines. The first one deals with identifying risk management activities throughout various selected ISO standards targeting management systems. It consists in the mapping of ISO 31000 with the following ISO selected standards: ISO Annex SL, ISO 9001, ISO 21500, ISO/IEC 20000-1 and ISO/IEC 27001 and ISO/IEC 27005. The second research line deals with driving integration for risk management activities in IT settings with the elicitation of management systems dedicated processes, and risk management specific processes. Terminology tables show the selected definitions applied to this research. Elementary statements are identified from ISO 31000. And finally requirement trees enable the identification of processes. The third research line deals with improving risk management processes throughout the IRMIS PRM and PAM enabling process assessment. For reaching this result, the Transformation process is applied to ISO 31000 and selected standards in order to fully develop the IRMIS PRM and PAM, with the help of goal trees for identified processes. The IRMIS PRM and PAM constitute the final outcome for an integrated risk management improvement framework in IT settings based on ISO standards.

Resumen

En la actualidad, la gestión de riesgos afecta a cualquier sector de la industria y a cualquier disciplina, como la gestión de calidad, la gestión de proyectos, la gestión de servicios y la gestión de la seguridad de la información. De la misma manera que en cualquier tipo de organización, la gestión de riesgos se hace muy patente en empresas de Tecnologías de la Información (TI) debido a la creciente complejidad de las aplicaciones, de los dispositivos y de las redes de comunicaciones. El mercado demanda, cada vez más, certificaciones para que las empresas puedan demostrar cómo satisfacen a sus clientes, incluyendo un enfoque de gestión de riesgos eficiente y eficaz. La Organización Internacional para la Estandarización (ISO) propone Estándares de Sistemas de Gestión (ESG), siendo el más popular la norma ISO 9001 y, en el dominio de las TI, por una parte, la norma ISO/IEC 20000-1 para el sistema de gestión de servicios de TI y, por otra, la norma ISO/IEC 27001 para el sistema de gestión de seguridad de la información. Con un enfoque basado en procesos y un pensamiento basado en el riesgo, la norma ISO 21500 aborda la gestión de proyectos. Estos cuatro estándares ISO antes mencionados, son de gran interés para muchos profesionales que trabajan en entornos de TI y que están preocupados por la integración de las actividades basadas en procesos, implementando mecanismos para establecer vínculos entre departamentos (tanto de TI como otros) con retos de gestión de riesgos por abordar. Por entornos de TI se deben entender empresas de TI y departamentos de TI, que abarcan tanto desarrollo como operaciones, con actividades basadas en proyectos y no basadas en ellos.

Tomando los estándares ISO como consenso internacional de buenas prácticas y con el objetivo de mejorar e integrar la gestión de riesgos en entornos de TI, se plantea la siguiente pregunta principal de la investigación: *"¿Cómo mejorar los procesos de gestión de riesgos en entornos de TI desde una perspectiva integrada y de sistemas de gestión en múltiples estándares ISO?"*. Algunos estudios previos han mostrado ciertas perspectivas de integración a nivel de estándares ISO y en marcos de mejores prácticas, realizando esfuerzos de armonización de los conceptos de estos múltiples marcos (incluyendo aspectos de gestión de riesgos). Estos estudios han sido realizados principalmente en las comunidades de ingeniería del software y en las de mejora de procesos de software. Existe un interés por integrar sistemas de gestión, en particular, de aquellos relacionados con la gestión de la calidad, la gestión ambiental y los ámbitos de la salud y de la seguridad, por razones de reducción de costes, eficiencia, eficacia y posicionamiento en el mercado. Existen investigaciones que han desarrollado diversos marcos y enfoques para facilitar la gestión integrada de riesgos, pero ninguna de ellas propone un camino unificado. En el ámbito de las TI, la ingeniería de software desempeña un papel importante, pero la gestión de riesgos no se aborda de un modo específico. Desde la perspectiva del rendimiento de los procesos, han surgido diversas iniciativas que han propuesto modelos de capacidad o/y de madurez con enfoques bastante heterogéneos. En este contexto, esta investigación pretende explorar la gestión de riesgos en entornos de TI desde el ángulo de los siguientes estándares ISO: ISO 31000, referencia internacional en gestión de riesgos, ISO Annex SL (estructura de alto nivel para los ESG), ISO 9001, ISO 21500, ISO/IEC 20000-1 e ISO/IEC 27001 (así como también ISO/IEC 27005 para entradas complementarias en gestión de riesgos de seguridad de la información). Se han analizado los estándares más relevantes con procesos de gestión de riesgos en modelos de evaluación de procesos, ya que proponen una descripción de los procesos de

gestión de riesgos. El proceso de gestión de riesgos, tal y como se aborda en la norma ISO 31000, es muy general. Hay poca diferencia entre los procesos de gestión de riesgos definidos en las normas anteriores y que, generalmente, mencionan un solo proceso de gestión de riesgos, sin descripciones detalladas sobre los diferentes aspectos de la gestión de riesgos: identificación, análisis, evaluación y tratamiento de los riesgos. Se han llevado a cabo algunos trabajos estrechamente relacionados con el ámbito de las TI en el sector médico, pero no abordaron la perspectiva del sistema de gestión; para facilitar la mejora del proceso de gestión de riesgos, adoptaron el mismo enfoque que el utilizado en este trabajo de investigación. Durante esta investigación, se ha trabajado siempre con la última versión de cada estándar seleccionado, y se ha realizado una selección de la terminología más apropiada relacionada con la gestión de riesgos existente en los estándares ISO.

Esta investigación se basa en los principios de *Design Science* para crear artefactos en entornos de TI. Se ha seguido un conjunto de seis actividades para crear un modelo de referencia de procesos (*Process Reference Model, PRM*) y un modelo de evaluación de procesos (*Process Assessment Model, PAM*) para procesos integrados de gestión de riesgos basados en estándares ISO (*Integrated Risk Management processes in IT settings, IRMIS, based on ISO Standards,*), con iteraciones e interacciones para mejorar la solución propuesta relacionada con el problema a ser resuelto. En primer lugar, en términos de identificación del problema y de motivación, los profesionales se enfrentan a múltiples retos en la industria con respecto a la mejora de la gestión de riesgos en el contexto de los estándares ISO en entornos de TI. Para definir los objetivos de la solución, los estándares ISO proporcionan el material con los requisitos y la orientación para definir un PRM y un PAM, así como conocimiento experto en la gestión de riesgos. Para diseñar y desarrollar los artefactos, se ha aplicado como enfoque sistemático un Proceso de Transformación de nueve fases. Para demostrar la resolución del problema, se ha realizado un primer ciclo de validación con expertos en gestión de procesos, de proyectos y de riesgos. La evaluación del PRM y PAM de IRMIS se ha realizado con un formulario de evaluación, complementado por el análisis de cada proceso, ya sea mediante la reutilización de las descripciones de procesos existentes en comités de la ISO, o mediante el análisis de expertos a través de revisiones de publicaciones por pares. Finalmente, se espera poder llevar a cabo una fase de comunicación que comprenda eventos con científicos y con profesionales, con publicaciones y con una atención particular y especial a la comunidad ISO, con la promoción del PRM y del PAM de IRMIS en comités técnicos específicos.

La contribución de esta investigación consiste en tres líneas principales. La primera trata sobre la identificación de actividades de gestión de riesgos en varios estándares ISO seleccionados que definen sistemas de gestión. Consiste en el mapeo de la norma ISO 31000 con los siguientes estándares ISO seleccionados: ISO Annex SL, ISO 9001, ISO 21500, ISO/IEC 20000-1 e ISO/IEC 27001 e ISO/IEC 27005. La segunda línea de investigación trata sobre la realización de la integración de las actividades de gestión de riesgos en entornos de TI con la obtención de procesos dedicados de sistemas de gestión y procesos específicos de gestión de riesgos. Las tablas de terminología muestran las definiciones que han sido aplicadas durante esta investigación. Las "Declaraciones elementales" han sido identificadas a partir de la norma ISO 31000. Y, finalmente, los "Árboles de declaración" han permitido la identificación de procesos. La tercera línea de investigación trata sobre la mejora de los procesos de gestión de riesgos, del PRM de IRMIS y de su PAM para la evaluación de procesos. Para alcanzar este resultado, se ha aplicado el Proceso

de Transformación a la norma ISO 31000 y a los otros estándares seleccionados, para poder desarrollar el PRM y el PAM de IRMIS, con la ayuda de “Árboles de objetivos” para los procesos identificados. El PRM y el PAM de IRMIS constituyen el resultado final de un marco integrado de mejora de la gestión de riesgos en entornos de TI basados en estándares ISO.

Resum

En l'actualitat, la gestió de riscos afecta qualsevol sector de la indústria i a qualsevol disciplina, com la gestió de qualitat, la gestió de projectes, la gestió de serveis i la gestió de la seguretat de la informació. De la mateixa manera que en qualsevol tipus d'organització, la gestió de riscos es fa molt patent en empreses de Tecnologies de la Informació (TI) a causa de la creixent complexitat de les aplicacions, dels dispositius i de les xarxes de comunicacions. El mercat demanda, cada vegada més, certificacions perquè les empreses puguin demostrar com satisfan als seus clients, incloent un enfocament de gestió de riscos eficient i eficaç. L'Organització Internacional per a l'Estandardització (ISO) proposa Estàndards de Sistemes de Gestió (ESG), sent el més popular la norma ISO 9001 i, en el domini de les TI, d'una banda, la norma ISO/IEC 20000-1 per al sistema de gestió de serveis de TI i, per l'altra, la norma ISO/IEC 27001 per al sistema de gestió de seguretat de la informació. Amb un enfocament basat en processos i un pensament basat en el risc, la norma ISO 21500 aborda la gestió de projectes. Aquests quatre estàndards ISO abans esmentats, són de gran interès per a molts professionals que treballen en entorns de TI i que estan preocupats per la integració de les activitats basades en processos, implementant mecanismes per establir vincles entre departaments (tant de TI com altres) amb reptes de gestió de riscos per abordar. Per entorns de TI s'han d'entendre empreses de TI i departaments de TI, que abasten tant desenvolupament com operacions, amb activitats basades en projectes i no basades en ells.

Prenent els estàndards ISO com a consens internacional de bones pràctiques i amb l'objectiu de millorar i integrar la gestió de riscos en entorns de TI, es planteja la següent pregunta principal de la investigació: *"Com millorar els processos de gestió de riscos en entorns de TI des d'una perspectiva integrada i de sistemes de gestió en múltiples estàndards ISO?"*. Alguns estudis previs han mostrat certes perspectives d'integració a nivell d'estàndards ISO i en marcs de millors pràctiques, realitzant esforços d'harmonització dels conceptes d'aquests múltiples marcs (incloent aspectes de gestió de riscos). Aquests estudis han estat realitzats principalment en les comunitats d'enginyeria del software i en les de millora de processos de software. Hi ha un interès per integrar sistemes de gestió, en particular, d'aquells relacionats amb la gestió de la qualitat, la gestió ambiental i els àmbits de la salut i de la seguretat, per raons de reducció de costos, eficiència, eficàcia i posicionament en el mercat. Existeixen investigacions que han desenvolupat diversos marcs i enfocaments per facilitar la gestió integrada de riscos, però cap d'elles proposa un camí unificat. En l'àmbit de les TI, l'enginyeria del software té un paper important, però la gestió de riscos no s'aborda d'una manera específica. Des de la perspectiva del rendiment dels processos, han sorgit diverses iniciatives que han proposat models de capacitat o/i de maduresa amb enfocaments força heterogenis. En aquest context, aquesta investigació pretén explorar la gestió de riscos en entorns de TI des de l'angle dels següents estàndards ISO: ISO 31000, referència internacional en gestió de riscos, ISO Annex SL (estructura d'alt nivell per als ESG), ISO 9001, ISO 21500, ISO/IEC 20000-1 i ISO/IEC 27001 (així com també ISO/IEC 27005 per a entrades complementàries en gestió de riscos de seguretat de la informació). S'han analitzat els estàndards més rellevants amb processos de gestió de riscos en models d'avaluació de processos, ja que proposen una descripció dels processos de gestió de riscos. El procés de gestió de riscos, tal com s'aborda en la norma ISO 31000, és molt general. Hi ha poca diferència entre els processos de gestió de riscos definits en les normes anteriors i que, generalment, esmenten un sol procés

de gestió de riscos, sense descripcions detallades sobre els diferents aspectes de la gestió de riscos: identificació, anàlisi, avaluació i tractament de els riscos. S'han dut a terme alguns treballs estretament relacionats amb l'àmbit de les TI en el sector mèdic, però no van abordar la perspectiva del sistema de gestió; per facilitar la millora del procés de gestió de riscos, van adoptar el mateix enfocament que l'utilitzat en aquest treball de recerca. Durant aquesta investigació, s'ha treballat sempre amb l'última versió de cada estàndard seleccionat, i s'ha fet una selecció de la terminologia més apropiada relacionada amb la gestió de riscos existent en els estàndards ISO.

Aquesta investigació es basa en els principis de *Design Science* per crear artefactes en entorns de TI. S'ha seguit un conjunt de sis activitats per crear un model de referència de processos (*Process Reference Model, PRM*) i un model d'avaluació de processos (*Process Assessment Model, PAM*) per a processos integrats de gestió de riscos basats en estàndards ISO (*Integrated Risk Management processes in IT settings, IRMIS, based on ISO Standards,*), amb iteracions i interaccions per millorar la solució proposada relacionada amb el problema a ser resolt. En primer lloc, en termes d'identificació del problema i de motivació, els professionals s'enfronten a múltiples reptes en la indústria pel que fa a la millora de la gestió de riscos en el context dels estàndards ISO en entorns de TI. Per definir els objectius de la solució, els estàndards ISO proporcionen el material amb els requisits i l'orientació per definir un PRM i un PAM, així com coneixement expert en la gestió de riscos. Per dissenyar i desenvolupar els artefactes, s'ha aplicat com a enfocament sistemàtic un Procés de Transformació de nou fases. Per a demostrar la resolució del problema, s'ha realitzat un primer cicle de validació amb experts en gestió de processos, de projectes i de riscos. L'avaluació del PRM i del PAM de IRMIS s'ha dut a terme amb un formulari d'avaluació, complementat per l'anàlisi de cada procés, ja sigui mitjançant la reutilització de les descripcions de processos existents en comitès de la ISO, o mitjançant l'anàlisi d'experts a través de revisions de publicacions per parells. Finalment, s'espera poder dur a terme una fase de comunicació que compregui esdeveniments amb científics i amb professionals, amb publicacions i amb una atenció particular i especial a la comunitat ISO, amb la promoció del PRM i del PAM de IRMIS en comitès tècnics específics.

La contribució d'aquesta investigació consisteix en tres línies principals. La primera tracta sobre la identificació d'activitats de gestió de riscos en diversos estàndards ISO seleccionats que defineixen sistemes de gestió. Consisteix en el mapatge de la norma ISO 31000 amb els següents estàndards ISO seleccionats: ISO Annex SL, ISO 9001, ISO 21500, ISO/IEC 20000-1 i ISO/IEC 27001 i ISO / IEC 27005. La segona línia d'investigació tracta sobre la realització de la integració de les activitats de gestió de riscos en entorns de TI amb l'obtenció de processos dedicats de sistemes de gestió i processos específics de gestió de riscos. Les taules de terminologia mostren les definicions que han estat aplicades durant aquesta investigació. Les "Declaracions elementals" han estat identificades a partir de la norma ISO 31000. I, finalment, els "Arbres de declaració" han permès la identificació de processos. La tercera línia de recerca tracta sobre la millora dels processos de gestió de riscos, del PRM de IRMIS i del seu PAM per a l'avaluació de processos. Per assolir aquest resultat, s'ha aplicat el Procés de Transformació a la norma ISO 31000 i als altres estàndards seleccionats, per poder desenvolupar el PRM i el PAM de IRMIS, amb l'ajuda d'"Arbres d'objectius" per als processos identificats. El PRM i el PAM de IRMIS constitueixen el resultat final d'un marc integrat de millora de la gestió de riscos en entorns de TI basats en estàndards ISO.

Acronyms

CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
C&MM	Capability and Maturity Models
COBIT	Control Objectives for Information and Related Technology
DSR	Design Science Research
GDPR	General Data Protection Regulation
GORE	Goal-Oriented Requirements Engineering
HLS	High Level Structure
IEC	International Electrotechnical Commission
ILNAS	Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services
ISMS	Information Security Management System
ISO	International Organization for Standardization
IRMIS	Integrated Risk Management in IT Settings
IT	Information Technology
ITIL	IT Infrastructure Library
ITSM	IT Service Management
JTC1	Joint Technical Committee 1
LIST	Luxembourg Institute of Science and Technology
MSS	Management System Standard
PAM	Process Assessment Model
PDCA	Plan-Do-Check-Act
PMBOK	Project Management Body of Knowledge
PRD	Process Risk Determination

PRM	Process Reference Model
RO	Research Objective
RQ	Research Question
SC	Sub-Committee
SE	Software Engineering
SMS	Service Management System
SPI	Software Process Improvement
SPICE	Software Process Improvement and Capability dEtermination
WG	Working Group

List of tables

Table 1. Articulation of PhD thesis	8
Table 2. List of Risk management processes in existing Process models fulfilling ISO/IEC 15504-330xx requirements for PRM & PAM	21
Table 3. Extract from ISO/IEC 33073: the Risk management process description.....	22
Table 4. Mapping of clauses between ISO 31000:2009 and ISO 31000:2018	23
Table 5: IRMIS PAM evaluation grid.....	33

List of figures

Figure 1: IRMIS PAM proposed list of processes.....	32
---	----

1. Introduction

This thesis is being submitted to the Universitat de les Illes Balears to satisfy the requirements for a Doctoral Thesis in the Doctoral Programme of Information and Communication Technology. It is entitled “Integrated Risk Management Process Improvement Framework in IT Settings based on ISO Standards”. It is a compendium of articles for the research contribution.

This chapter is divided into four parts. First, history and background are explained: a process assessment framework named TIPA is described as the foundations of this PhD thesis, as well as the standardization background. Secondly, the motivation of the work is presented, followed by the research objectives, and finally the research contributions with the articulation of the PhD thesis.

1.1 History and background

1.1.1 The TIPA® Framework

This PhD thesis has foundations resulting from many years of applied research in the domain of process assessment and improvement. This long term applied research sets the ground of this PhD thesis: a process assessment framework has been developed in the Luxembourg Institute of Science and Technology (LIST, previously known as Public Research Centre Henri Tudor) in Luxembourg; the author of this PhD thesis has been at the origin of this framework and has been leading a team on these topics since 2003. This framework has been branded TIPA® (TIPA is a registered trademark). It has been designed and populated with various artefacts since 2002. There was an initial founding paper for stating the problem to be solved, collected from empirical evidence in companies [1]. Back in 2002, it was reported that many process assessments were carried out for “*software processes by making use of IEC/ISO 15504*”[2]; it was noticed several times that in IT organizations covering both software developments and IT operations, “*assessed organizations were also using ITIL*” (Information Technology (IT) Infrastructure Library [3] in the IT Service Management (ITSM) domain), ITIL being the de facto standard for ITSM. *Beyond the comparison that can be made between both standards, it has been a precious experience to analyse and collect information coming directly from day-to-day users of the standards.*” [1]. Then the following matter was raised as a subject of research: “*Does the combined use of ITIL and IEC/ISO 15504 truly increases effectiveness and efficiency and can be adapted to the need of flexibility of today’s organizations?*” [1]. In order to address this research question, a Process Reference Model (PRM) and a Process Assessment Model (PAM) based on ITIL was developed, fulfilling ISO/IEC 15504 requirements for designing process models enabling process assessments. From this initial problem statement, a Design Science approach has been followed with various iterations. The first ones were performed between 2003 and 2009 as explained in [4]: “*TIPA, was designed as a solution to reduce the cost for assessing ITSM processes and for companies aiming at improving them. This solution was mainly based on a methodological framework (process models; assessment methodology and associated tools such as questionnaires, templates and case study examples; training courses for assessors) enabling the assessment of ITSM processes.*”

In this process assessment and improvement applied research context, some works were particularly targeting the engineering of process models. As stated in [4], the purpose was *“to design and manage an ISO/IEC 15504 compliant process model (validation and traceability) fulfilling the stakeholders’ requirements and needs, and to provide a knowledge base supporting uses of the model... By using a rigorous and systematic approach for developing PRMs and PAMs, it provides a very structured and trusted basis for process improvement. Then it can be valuable inputs for combining process modeling and assessment with the help of a support tool, within an improvement approach contextualized to an organization... In the context of TIPA, the use of this systematic approach for developing process models based on ITIL V2 in a first time, and later on ISO/IEC 20000-1 [5] was very useful and helped to gain structured feedback on the quality of the models. This theoretical feedback is completed by companies using the TIPA’s framework, and by CRP Henri Tudor engineers participating in ISO standardization works.”* In conclusion in [4], the innovation loop was shown. It was in a context of research-action in the Service Science, with a multi-disciplinary approach. The research centre developed an innovation management governance model which guided and structured works: it was the case for designing process models and gaining maturity in this activity. For designing process models (PRMs and PAMs), a Goal-Oriented Requirements Engineering (GORE) technique was used. Back in 2008, the systematic way used to design PRMs and PAMs (Transformation process) was documented, with an illustration on the ISO/IEC 20000-1 PRM/PAM design [6]. These works scientifically grounded a main asset of the TIPA framework: the process models. Various applications of the Transformation process have been performed and published [7, 8, 9]; these works for designing capability process models have been extended to the notion of organizational maturity model design in [10, 11]. Thereafter joint works in the domain of Project management with the design of the Project Management SPICE PRM and PAM [12] were also initiated.

For performing process assessment, a documented process assessment process is required. Then beyond the process models, the TIPA Framework includes a process assessment method. The TIPA method was formalized in a published handbook [13]. This is another main asset of the TIPA Framework as it helped designing the training courses for TIPA Assessors and Lead Assessors course. Moreover the TIPA for ITIL instance of the TIPA Framework has been transferred to the market as a commercial partner is selling the TIPA for ITIL training courses and promoting its use with the help of a Toolbox provided by LIST.

Extensive works have been performed in the context of the TIPA Framework. The author of this PhD thesis has been involved in all of them. The TIPA Framework gained maturity with publications relating the developed experience [14, 15]. From a Design Science perspective, more iterations have been performed and the TIPA Framework has been analysed from this perspective in [16].

As a summary of previous information, the TIPA Framework was initiated with the idea of applying the requirements and guidance of the ISO/IEC 15504 process assessment standards series to the ITIL® de facto standard with ITSM best practices. This initiative was targeting end-users and consultants in order to support them in the ITIL process improvement with a *“standard-based, objective, repeatable and trustful method”* [16]. Over time, the TIPA Framework has been applied to various domains and is composed of a set of artefacts, with a customization to the targeted domain when necessary:

- Process models: Process Reference Models and Process Assessment Models. These PRMs and PAMs are the result of a transformation [6] from the set of requirements or statements or practices from a source document (best practices standard, ISO standard with requirements or statements of guidance, regulation...) into a set of processes described in terms of purpose and outcomes (in the PRM) and assessment indicators (associated with a purpose and outcomes for each process, and providing base practices, work products and resources) for the process dimension, and a capability measurement framework providing measurable capability levels (in the PAM);
- Process assessment method: the TIPA process assessment method documents the assessment process, and uses as inputs the processes documented in the TIPA process models. The method is documented in the published TIPA handbook [13];
- Toolbox: questionnaires, templates, checklists, rating sheets,... which support each phase of the TIPA process assessment method;
- Assessor & Lead Assessor training courses and the associate professional certification scheme.

After a second iteration from Design Science perspectives on the TIPA framework [16], the TIPA team analysed the deployment of the TIPA Framework instantiated to ITIL and transferred to the market. This incremental innovation provides high quality process descriptions within the process models with a sound basis for assessing and improving practices. Nevertheless the *“uniqueness of the ITIL-based proposed solution and the qualities of the TIPA for ITIL services for assessing and improving ITSM processes have to be strengthened.”* [16]. Future works and perspectives in IT service quality were considered. Actually the TIPA Framework has been expanded and additional components were planned. A Software-as-a-Service tool development has been initiated in order to support the TIPA Framework (to embed process models and support the TIPA method and toolbox, to gain time and reduce costs, to improve assessability, effectiveness and efficiency of process assessments). From a TIPA Factory perspective, additional process models were developed (whether developed by LIST or by others such as in ISO) and populate the process model library; more connections and interoperability between models can be operated.

In this overall TIPA Framework context, an Integrated Risk Management process model was foreseen. It can be the opportunity to provide an integrated process view from a governance, risk management and compliance (GRC) perspective for quality, project, IT services and information security management aspects.

1.1.2 Standardization background

In LIST, the author has been studying and using the ISO standard on Process Assessment (ISO/IEC 15504 series, and its revision within the ISO/IEC 330xx series) since the mid-nineties for assessing Software Engineering (SE) processes in the first place. The author and other LIST experts have participated to Trial phases of the standard implementation at the end of the nineties; they joined the standardization community at the beginning of the years 2000 for push/pull actions and taking maximum benefits for innovation and competitive advantage in companies. They were fast in understanding the interest of

applying the generic framework for process assessment to other fields of activity than SE, such as IT Service Management, but also for non IT domains: Knowledge Management, Operational Risk Management (ORM), Know Your Customer/Anti-Money Laundering, and Accreditation.

For more than 15 years, the author of this PhD thesis has been very actively involved in standardization activities in ISO, in Sub-Committees (SC) such as ISO/IEC JTC1 SC7 (Software and Systems Engineering) and ISO/IEC JTC1 SC40 (IT Service Management and IT Governance).

As stated by ISO in [17], ISO/IEC JTC1 “*SC7 delivers standards in the area of software and systems engineering that meet market and professional requirements. These standards cover the processes, supporting tools and supporting technologies for the engineering of software products and systems. [...] SC7, whose scope is Software and Systems Engineering, can thus be described as a horizontal committee who produces generic standards that are technology agnostics and independent of the application domain. These standards are principally focused on process models and good practices (Methods and techniques).*” In SC7, 17 working groups (WGs) actively develop new standards and maintain/revise existing standards. As previously mentioned, the author has been particularly involved in activities dedicated to process assessment in WG10.

The author has also been involved in ISO/IEC JTC1 SC40 which deals with IT Service Management and IT Governance. As stated in [18], SC40 develops “*standards, tools, frameworks, best practices and related documents for IT Service Management and IT Governance, including areas of IT activity such as audit, digital forensics, governance, risk management, outsourcing, service operations and service maintenance, but excluding subject matter covered under the scope and existing work programs of JTC 1/SC27 and JTC 1/SC38.*” (SC27 covers IT security techniques and SC38 covers Cloud computing and distributed platforms). There are four active WGs in SC40 and the author has been particularly involved in WG2 dealing with Maintenance and development of ISO/IEC 20000 - Information technology - Service management.

So the author has been representing Luxembourg at the international level and positioning Luxembourg in general and LIST’s works in particular with significant impacts on TIPA results and overall TIPA-related networks. At the beginning of 2014, the author became President of the ISO/IEC JTC1 SC40 for the national technical mirror committee, after having been the SC7 Luxembourg President for nine years. The author was editor of the ISO/IEC 20000-4 standard (published in 2010) for an ITSM Process Reference Model. In 2014, the author received the Luxembourg standardization delegate award from the national standardization body ILNAS (Institut Luxembourgeois de la Normalisation, de l’Accréditation, de la Sécurité et qualité des produits et services).

1.2 Motivation of work

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. IT 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 pervasive and essential for any business. Risk management is part of these key challenges and is related to a multitude of domains, for IT and non-IT concerns. In IT settings, many activities are strongly related to risk management: project management, information security and ITSM to quote the main domains. Risk is defined in [19] 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)”*. 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 [20] 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”*.

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 (MSSs) such as the ISO/IEC 27001 [21] for information security or the ISO/IEC 20000-1 [5] for ITSM. They may also need to integrate these IT related standards with more general ones such as the ISO 9001 [22] 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.

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 ISO and on the market, there are several published Process Reference Models (PRM) and Process Assessment Models (PAM) in different kinds of domains [23, 24, 25, 26]; these various initiatives are based on the ISO Process assessment standard series concepts [2, 27]; they rely on a very structured and systematic approach for process assessment and guided process improvement.

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. ISO definition of standard is as follows: *“Document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.”* AFNOR, the French National Body for Standardization, has published a survey showing the benefits of standardization for the economy, with visible benefits on companies' results [28]. The ISO continuously promotes standardization benefits [29] and MSSs [30]. Every year, ISO performs a survey [31] of certifications to MSSs. The 2017 results show again that ISO 9001 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 (Service management system requirements), after recommendations from international accreditation and certification experts that are consulted annually. Despite the fact that ITIL [3] remains the de facto standard in ITSM, ISO/IEC 20000-1 is still 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 [32]. Regarding Project management, we can quote that ISO 21500 (Guidance on Project management [33]) 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 (PDCA) 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 QMSs. 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. By IT settings, the author mean IT companies and IT departments, covering both development and operations sides, with projects and non-projects based activities. These IT-related and non-IT standards are significant for many companies and were reported back to the author by practitioners. Addressing risk management in some market-significant ISO standards from integration and improvement perspectives in IT organizations appeared as key challenges. The author made the assumption that an integrated risk management approach for IT Organizations will benefit organizations by being based on ISO standards which represent international consensus. This assumption is supported by market demand for ISO 9001, ISO/IEC 27001 and ISO 20000-1 as popular standards for certification of management systems, completed by ISO 21500 because project management is always a critical process in IT organizations. As ISO 31000 [34] is the ISO international reference for Risk management, this standard is providing an Ariane's thread for these research works, as explained in the State-of-the-Art (see chapter 0). So these standards are the ground material of the research. This PhD thesis is aiming at exploring key challenges and at demonstrating how research objectives (next paragraph) can be fulfilled with research contributions (structured and explained in paragraph 1.4).

1.3 Research objectives

With the previously described context, background and motivation, the overall 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, based on ISO standards.

In this context, the main research question is:

how to improve risk management processes in IT settings from an integrated and management system perspective in multiple ISO standards?

Several sub-questions are investigated with their respective research objective:

- *RQ1: How to identify risk management activities throughout various selected ISO standards targeting management systems?*
 - *RO1: to investigate and compare risk management activities throughout selected ISO standards targeting management systems*
- *RQ2: How to drive integration for risk management activities in IT settings?*
 - *RO2: to show that a centralized and management system approach based on processes contributes to integration in a process-centric risk management mindset in IT settings.*
- *RQ3: How to improve risk management processes?*
 - *RO3: to propose means to improve Risk management processes in IT settings, with a structured, integrated, interoperable, assessable, effective and efficient way (these criteria guide our applied research).*

The intended outcomes of this research are represented by two main artefacts according to a Design Science approach which supports the research approach:

- Integrated Risk Management in IT Settings (IRMIS) Process Reference Model (PRM) & Process Assessment Model (PAM)

and by a set of intermediary artefacts that are necessary for the design of the two main artefacts:

- Mapping of ISO 31000 with ISO selected standards
- Terminology tables showing the selected definitions applied in this PhD thesis
- Transformation process applied to ISO 31000 and selected standards for designing the IRMIS PRM and PAM
- Elementary statements identified from ISO 31000
- Requirement trees and Goal trees for identified processes

The research contributions architecture with the combination of main and intermediary artefacts are explained in the next paragraph.

1.4 Research contributions

The contributions of this PhD thesis are articulated among the various chapters:

- Chapter 2 presents the State-of-the-Art of the PhD thesis;
- Chapter 3 presents the Research approach according to Design Science;
- Chapter 4 includes the major publications representing the research contribution of this Compendium of articles;
- Chapter 5 presents the Discussion and Conclusion of the PhD thesis;
- Chapters 6 to 9 provides some intermediary and major artefacts in annexes;
- finally Chapter 10 lists the references.

Table 1. Articulation of PhD thesis

Main research question: <i>How to improve risk management processes in IT settings from an integrated and management system perspective in multiple ISO standards?</i>			
Research sub-questions	<i>RQ1. How to identify risk management activities throughout various selected ISO standards targeting management systems?</i>	<i>RQ2. How to drive integration for risk management activities in IT settings?</i>	<i>RQ3. How to improve risk management processes?</i>
State-of-the-Art (chapter 2)	Overview of targeted ISO standards (§ 2.3)	Harmonization in Software Engineering and Software Process Improvement (§ 2.2.1) Integrating management systems standards (§2.2.2) Integrated risk management in literature (§ 2.2.3) Risk management in IT and software contexts (§ 2.2.4) ISO standards terminology for risk management (§ 2.5)	Process models, process assessment and process improvement (§ 2.2.5) Study of relevant standards with risk management processes in PAMs (§ 2.4)
Artefacts developed / obtained	Mapping of ISO 31000 with ISO selected standards (in paper C1)	Terminology tables showing the selected definitions applied in this PhD thesis Elementary statements identified from ISO 31000 Requirement trees with identification of processes	Transformation process applied to ISO 31000 and selected standards Goal trees for identified processes IRMIS PRM & PAM

Main Research Contributions: Papers* (chapter 4)	Paper C1	Papers C2 & C3	Papers C2 & C3
Other papers*: - published during the PhD period - related to the PhD thesis	Papers C4, C5 & C8	Paper C7	Papers C6, C9 & C10

*: All papers with ID "Cn" are referenced in the "List of Manuscripts", page vii.

2. State-of-the-Art

Various facets of integrated risk management, management systems, significant ISO standards in IT settings, have been investigated in the next four paragraphs in order to address research questions. These four paragraphs are covering the following aspects:

- Integration perspectives in 2.1;
- Overview of ISO standards in 2.2;
- Study of relevant standards with Risk management process(es) in PAMs in 2.3;
- ISO standards terminology for risk management in 2.4.

2.1 Integration perspectives

In order to investigate integration perspectives, a first exploration tackles harmonization in SE and SPI. Then the ways to integrate management systems standards are examined before studying integrated risk management in literature. Risk management in IT and software contents is also studied, as well as process models, process assessment and process improvement.

2.1.1 Harmonization in Software Engineering and Software Process Improvement

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 engineering SC7 in ISO/IEC JTC1 is aiming at proposing an ontology to unify ISO SE standards [35]. 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 [36]. Harmonizing software development processes is also an important concern and mappings between processes and project settings have been investigated from the situational factors angle [37]. 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 [38] as well as for the ISO/IEC 29110 with the ITMark certification schema assessing software processes of software companies [39].

More generally, harmonizing approaches have been proposed for quality frameworks and standards addressing Software Process Improvement (SPI) practices; we can quote research works with case studies where ISO 9001 and Capability Maturity Model Integration for Development (CMMI-DEV) have been harmonized and supported [40]. 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 [41] 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, Capability Maturity Model Integration (CMMI), ISO/IEC 12207 and ISO/IEC 90003, ITIL, Project Management Body of Knowledge (PMBOK) and Control Objectives for Information and Related Technology (COBIT), ISO/IEC 27001 and ISO/IEC 20000-1. This research team also proposes a process improvement approach based on multiple models [42, 43].

2.1.2 Integrating management system standards

From the integration perspective, integrating management systems has been a topic of interest in research and industry for many years now [44, 45]. This has been particularly true for quality management, environmental management and health and safety domains [31]. It has been more and more necessary to integrate these systems for cost reductions, efficiency, effectiveness, and market positioning.

The integration of management systems, in particular from the ISO 9001 perspective, has been considered in many works. In the IT domain, with the first publication in 2005 of the ISO/IEC 20000-1 and ISO/IEC 27001, new MSSs appeared on the international scene, respectively for ITSM and Information Security. The latest ISO survey [31] 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 [46] 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 in [46] 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 [47] 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.

Some integration models and approaches have been tackled [48, 49] with a model proposition for integrating management systems [50], mainly driven by the ISO 9001 QMS implementation in a large number of companies.

As MSSs interest increased, ISO published in its Directives an annex named *“High-level structure (HLS), identical core text, common terms and core definitions”* for MSS [20]. 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 [21]. The ISO 9001 has been upgraded in its last revision of 2015 [22]. The ISO/IEC 20000-1:2011 [5] standard was partially aligned and is aligned in its revised version published in 2018 [51].

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 [6, 9]. These works have been proposed to ISO and were incorporated within PRMs and PAMs for Information Security [52] and ISO 9001, and potentially for ISO/IEC 20000-1. The 2018 plenary international meeting for ISO/IEC JTC1 SC7 WG10 decided to launch the revision of the PRM (ISO/IEC 20000-4 [53]) and the PAM (ISO/IEC 15504-8 [25]) based on ISO/IEC 20000-1.

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 [54] 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) [55]. Several approaches target methodologies for implementing risk management; we can cite [56] for Risk management in ISO/IEC 27001; we can also mention specific risks such as cloud computing ones [57]. 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 [33] 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 author [58, 12] where a process-oriented organization can benefit from this high value structure for process assessment and process improvement purposes.

2.1.3 Integrated risk management in literature

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. Integrated risk management addresses risks at very different levels in the organization, including strategy and tactics, and covering both opportunity and threat [59].

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 Haines [60]. The role of human resource development and improvement in risk assessment is given special attention. The framework from Lyytinen et al. [61] 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. [62] developed a framework with four major components: risk identification, risk analysis, risk-reducing measures and risk monitoring. Riskit, a method developed by Kontio [63] 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 [64] 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 [65] 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 [66] 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 [67] for the Risk management process of the PAM ISO/IEC 15504-5 [67]. Recently, a development of a Maturity Model for risk management has been performed [68], based on the ISO 31000 standard version of 2009. The authors propose an analysis of existing maturity models related to risk management; they selected some inputs (i.e. 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 this PhD thesis' research.

2.1.4 Risk management in IT and software contexts

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 [69]. 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 [70] 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. [71] 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, SE plays a significant part where risk management is also considered from various perspectives: embedded in project management, included in SPI approaches or part of software and/or system life cycle. The SPI Manifesto [72] "*gives expression to state-of-the-art knowledge on SPI*" with three values (people, business, change), further elaborated into ten 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, risk management must be present. There is an ISO standard favoring risk management in life cycle processes: ISO/IEC/IEEE 16085 [73]: "*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 QMS 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.

2.1.5 Process models, process assessment and process improvement

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 [74]. Becker et al. explored various C&MM [75] and Pöppelbuß some design principles for useful maturity models [76]. As the Capability Maturity Model (CMM) was first developed in the SE community and as the Process Assessment have its own ISO standard [27] with requirements for developing PRMs and PAMs [77], different process models were developed in this area. A Brazilian initiative developed a framework for engineering process models in the software domain [78]. In the same vein, another Austrian initiative developed methodological support [79]. Several process models for IT and non-IT works have been developed in Luxembourg, in an R&D initiative encompassing the TIPA Framework [15] with PRMs and PAMs for ITIL and Operational risks [80].

In the years 2000, maturity models, process assessment and improvement frameworks were very popular, such as CMMI [81] and ISO/IEC 15504 standards [82]. 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 [83], based on Medical Device regulatory requirements and CMMI. PAMs such as the PAM ISO/IEC 15504-8 [25], and the ISO/IEC 27001 Information Security one recently published by ISO [52], 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 [84]; it enables the comparison of integrated systems implemented in different companies or contexts.

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 PAMs based on MSSs. As previously mentioned, it is the case for Information security management (ISO/IEC 33072 [52]), and ITSM (ISO/IEC 15504-8 [25]), but also for quality management based on ISO 9001 (ISO/IEC 33073 [85]). 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 Organisations can assess risk management process capability considering the requirements of IEC 80000-1 which is the application of risk management to IT-networks [100]. This risk management life cycle process model provide 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 favour a process approach and management system mechanisms, reproducing the way introduced by the author in publications (see C1 in Chapter 4).

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 [41]. 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, section 2.4 analyses and settles the terminology that has been used.

2.2 Overview of ISO standards

Considering the gained experience by the author from the various domains, this PhD thesis intends to explore risk management in IT settings from the angle of the following ISO standards: ISO 31000 as main theme, and ISO Annex SL, ISO 9001, ISO 21500, ISO/IEC 20000-1, ISO/IEC 27001 as particular views from an IT setting perspective. Other standards are presented as they are interesting to be considered, such as the ISO 22301 Societal security - Business continuity management systems – Requirements [86], ISO 90006 Guidelines for the application of ISO 9001:2008 to IT service management and its integration with ISO/IEC 20000-1:2011 [87], ISO/IEC 12207 Software lifecycle processes [8886] and ISO/IEC 15288 System lifecycle processes [89] are not considered as they are not directly targeting a PDCA neither a management system approach. ISO/IEC 27005 is used to complement the ISO/IEC 27001 views.

As previously mentioned, ISO performs every year a survey of certifications to MSSs [31]. For ISO 9001, there has been 1.058.504 certificates in 2017, 39.501 certificates for ISO/IEC 27001 (increase of 19% compared to 2016) and 5.5005 for ISO/IEC 20000-1 which was introduced in 2015 in this survey (increase of 10% compared to 2016).

2.2.1 ISO 31000:2018 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.

ISO 31000 has been revised. Several discussions were going on in the international community involved in its revision. There was a debate on terminology as the definition of Risk is not perceived equally

in all countries [90]. 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 remains a principles standard, without certification as a target. ISO 31000 has been republished at the beginning of 2018 and the author considers this latest version for her R&D works, meaning a revision of initial works of this PhD thesis for encompassing changes. The main changes of this latest 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 to the previous version, because they are already part of the ISO Guide 73 [19].

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 [91].

As quoted by Jason Brown at ISO, Chair of technical committee ISO/TC 262 on risk management that developed the standard: *“The revised version of ISO 31000 focuses on the integration with the organization and the role of leaders and their responsibility. Risk practitioners are often at the margins of organizational management and this emphasis will help them demonstrate that risk management is an integral part of business.”*. Regarding the PhD’s research objectives, ISO 31000 is the appropriate standard candidate for driving the comparison of risk management from a generic perspective in various ISO standards, and for being the main reference and Ariane’s thread for risk management.

2.2.2 ISO/IEC Directives Part 1 and Consolidated ISO Supplement – 2018 (9th edition) - Annex SL: Proposals for Management System Standards – Appendix 2: High level structure

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 MSSs and enables 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 HLS to all MSSs, and then naturally targets risk management on a consistent way. As quoted in the following paragraphs, ISO 9001, ISO/IEC 27001 and ISO/IEC 20000-1 are aligned with the HLS. The HLS is relevant for this PhD thesis works.

2.2.3 ISO 9001:2015 Quality management systems - Requirements

The flagship standard ISO 9001 providing requirements for QMSs has been revised and published in September 2015. This 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 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.”*.

This standard is selected as a relevant standard for the PhD thesis. It is an MSS and follows the HLS.

2.2.4 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 that the PMBOK Guide® [92] had a great influence on the ISO 21500 standard development. In this context, as in PMBOK, risk management is 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.

This standard is selected as a relevant standard for the PhD thesis. It is not a MSS but follows the HLS principles of an MSS with a PDCA approach.

2.2.5 ISO/IEC 20000-1:2018 Part 1: 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 published latest version of ISO/IEC 20000-1 (2018) is fully aligned with the HLS, with requirements related to risk management, coming from the HLS. ISO 31000 is cited as a reference for generic risk management.

This standard is selected as a relevant standard for the PhD thesis. It is an MSS and follows the HLS.

2.2.6 ISO/IEC 27001:2013 Information security management systems - Requirements

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. ISO/IEC 27005 [55] provides guidelines for information security risk management and complements ISO/IEC 27001.

This standard is selected as a relevant standard for the PhD thesis. It is an MSS and follows the HLS.

2.2.7 ISO 22301:2013 Societal security - Business continuity management systems – Requirements

As stated on the ISO web site, *“ISO 22301:2012 specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.”*

The requirements specified in ISO 22301 are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity. ISO 22301 is aligned with the HLS.

This standard is not selected as a relevant standard for the PhD thesis. It is an MSS and follows the HLS, but was not particularly demanded by the market for IT settings.

2.2.8 ISO/IEC 90006:2013 Guidelines for the application of ISO 9001:2008 to IT service management and its integration with ISO/IEC 20000-1:2011

As stated on the ISO web site: *“ISO/IEC TR 90006:2013 provides guidelines for the application of ISO 9001:2008 to service management for IT services. Examples provided in the guidelines are for service management of IT services.*

Additionally, ISO/IEC TR 90006:2013 provides guidelines for the alignment and integration of a QMS and SMS in organizations where services are being delivered to internal or external customers. The guidelines about integration provided can be applicable to a scope including IT services and other non-IT services as required.”

This guideline standard is aiming at explaining the requirements of ISO 9001 with an application view related to service management and an integration one towards ISO/IEC 20000-1.

This standard is not selected as a relevant standard for the PhD thesis as it is just providing guidance, but it can help with interesting insights for those companies wishing to align ISO 9001 and ISO/IEC 20000-1.

2.2.9 ISO/IEC/IEEE 12207:2017 Systems and software engineering – Software life cycle processes

As stated on the ISO web site: *“ISO/IEC/IEEE 12207:2017 also provides processes that can be employed for defining, controlling, and improving software life cycle processes within an organization or a project.*

The processes, activities, and tasks of this document can also be applied during the acquisition of a system that contains software, either alone or in conjunction with ISO/IEC/IEEE 15288:2015, Systems and software engineering - System life cycle processes.”

This standard is a very important one in the SE community. It is not selected as a relevant standard for the PhD thesis as it is just proposing a single risk management process, and is not structured as a management system.

2.2.10 ISO/IEC/IEEE 15288:2015 Systems and software engineering – System life cycle processes

As stated on the ISO web site, *“ISO/IEC/IEEE 15288:2015 establishes a common framework of process descriptions for describing the life cycle of systems created by humans. It defines a set of processes and associated terminology from an engineering viewpoint. These processes can be applied at any level in the hierarchy of a system's structure.”*

This standard is not selected as a relevant standard for the PhD thesis as it is just proposing a single risk management process, and is not structured as a management system approach.

2.3 Study of relevant standards with Risk management process(es) in PAMs

A lot of work has targeted Risk management in various domains. C&MM are amongst them. A recent paper presenting the LEGO approach (Living EnGineering prOcess: approach to process improvement) to achieve a meta-model on Risk Management merging various sources, includes a survey on Risk management C&MM which has shown and compared their respective approaches [93]. They were different in structure and levels. To ensure integration and consistency, and to align with market demands and pressures related to certifications, this PhD's research focuses on PRMs and PAMs fulfilling ISO/IEC 15504/330xx requirements on Process assessment and encompassing management systems principles. The economic benefits of standards is demonstrated in the industry [94], in particular with ISO certifications such as the most popular one: ISO 9001.

The author has studied existing and available PRMs & PAMs related to Risk management in C&MM context, based on publicly available ISO/IEC 15504/330xx. Table 2 lists these Risk management processes and their source.

Table 2. List of Risk management processes in existing Process models fulfilling ISO/IEC 15504-330xx requirements for PRM & PAM

Process model	Name of the Risk management related process(es)
ISO/IEC 15504-5:2012 – Part 5: An exemplar software life cycle process assessment model [67]	MAN.5 Risk management
ISO/IEC 15504-6:2013 – Part 6: An exemplar system life cycle process assessment model [95]	PRJ.5 Risk management
ISO/IEC 15504-8:2012 – Part 8: An exemplar process assessment model for IT service management [25]	SMS.6 Risk management
Enterprise SPICE (ISO/IEC 33071:2016 – An integrated process capability assessment model for Enterprise processes) [96]	GVM.9 Risk management
ISO/IEC 33072:2016 – Process capability assessment model for information security management [52]	COM.11 Risk and opportunity management
ISO/IEC 33073:2017 – Process capability assessment model for quality management [85]	COM.11 Risk management
ISO/IEC 30105-2: 2016 – Information technology – IT Enabled Services-Business Process Outsourcing (ITES-BPO) lifecycle processes – Part 2: Process assessment model (PAM) [97]	ENB1 Risk management
Automotive SPICE Process Assessment Model [98]	MAN.5 Risk management
COBIT Process Assessment Model (PAM): Using COBIT 5 [99]	EDM03 Ensure risk optimisation APO12 Manage risk

According to these processes, the risk management process, as addressed by the ISO 31000 standard, is very general. There is little difference among these processes, where risk identification is performed, and then analysis and evaluation, from the risk assessment perspective, and finally risk treatment. There is not much detail in each of these PAM. As illustration in Table 3, extracted from the latest published standard ISO/IEC 33073 Process Capability Assessment Model for quality management [85], the Risk management process is described:

Table 3. Extract from ISO/IEC 33073: the Risk management process description

Process ID	COM.11
Name	Risk management
Purpose	The purpose of Risk Management is to identify, analyse, evaluate, treat and monitor risks.
Outcomes	As a result of successful implementation of this process: <ol style="list-style-type: none"> 1. Risks are identified. 2. Identified risks are analysed. 3. Risks are evaluated against defined criteria. 4. Risks are selected for treatment. 5. Selected risks are treated.

In addition to processes classified in Table 2, some closely related works have been performed in the medical IT networks domain with a PRM and PAM for improving risk management, in order to allow Healthcare Delivery Organisations to assess the capability of their risk management processes against the requirements of IEC 80000-1 (application of risk management to IT-networks incorporating medical devices) [100]. There are 14 processes for different aspects of the life cycle risk management. In this process model, there are four processes dedicated to the risk management itself: Medical IT Network Risk Management, Risk Analysis & Evaluation, Risk Control, and Residual Risk. This approach is targeting the medical sector with a particular objective of contribution to ISO 80000-1 but with a common overall goal with our works for improving risk management processes. The author nevertheless addresses management systems from various selected ISO standards perspectives in an IT Organizations mindset.

It is also relevant to highlight that there is an important aspect in implementing standards: its version. Standards are continuously revised, when relevant. There is an official standard lifecycle at ISO, and once published, there is a systematic review every five years. As stated on ISO web site, *“Systematic Review provides valuable information on the global relevance of the standard and ensures that the ISO catalogue is up-to-date. It is also currently the only systematic way for the ISO Central Secretariat to collect information on the use of ISO standards and their national adoption”*. All along this PhD thesis, the author checked the versions of standards and decided to consider the latest versions; some reworks have been performed in order to keep the alignment in mappings and orientations of the PhD work. This enabled to have updated views and alignment. So with the ISO 31000 as the main driver of the PhD’s work, adopted the latest version was adopted. The author checked the alignment of clauses between ISO 31000:2009 and ISO 31000:2018 in Table 4: they are totally aligned with a few adjustments, notably for the terminology and some concepts which became more generic (i.e. *“4.2 Mandate and commitment”*

became “5.2 Leadership and commitment”, “4.3.2 Establishing risk management policy” became “5.3.2 Articulating risk management commitment”, “4.3.3 Accountability” became “5.3.3 Assigning organizational roles, authorities, responsibilities and accountabilities”, “4.3.5 Resources” became “5.3.4 .Allocating resources”, a new clause labelled “5.5 evaluation” appeared, and “5.7 Recording the risk management process” became “6.7 Recording and reporting”.

Table 4. Mapping of clauses between ISO 31000:2009 and ISO 31000:2018

ISO 31000:2009		ISO 31000:2018	
4.2	Mandate and commitment	5.2	Leadership and commitment
4.3.1	Understanding of the organization and its context	5.3.1	Understanding of the organization and its context
4.3.2	Establishing risk management policy	5.3.2	Articulating risk management commitment
4.3.3	Accountability	5.3.3	Assigning organizational roles, authorities, responsibilities and accountabilities
4.3.4	Integration into organizational processes	5.2.2	Integrating risk management
4.3.5	Resources	5.3.4	Allocating resources
4.3.6	Establishing internal communication and reporting mechanisms	5.3.5	Establishing communication and consultation
4.3.7	Establishing external communication and reporting mechanisms	5.3.5	
4.4.1	Implementing the framework for managing risk	5.4	Implementation
		5.5	Evaluation (NEW)
4.6	Continual improvement of the framework	5.6	Improvement
5.1	General	6.1	General
5.2	Communication and consultation	6.2	Communication and consultation
5.3.2	Establishing the external context	6.3.1	Establishing the context – General
5.3.3	Establishing the internal context	6.3.2	Establishing the context - Defining the purpose and scope
5.3.4	Establishing the context of the risk management process	6.3.3	Establishing the context – Context

ISO 31000:2009		ISO 31000:2018	
5.3.5	Defining risk criteria	6.3.4	Defining risk criteria
5.4.2	Risk identification	6.4.2	Risk identification
5.4.3	Risk analysis	6.4.3	Risk analysis
5.4.4	Risk evaluation	6.4.4	Risk evaluation
5.5.1	General - Risk Treatment	6.5	Risk treatment
5.5.2	Selection of risk treatment options	6.5.2	Selection of risk treatment options
5.5.3	Preparing and implementing risk treatment plans	6.5.3	Preparing and implementing risk treatment plans
5.6	Monitoring and review	6.6	Monitoring and review
5.7	Recording the risk management process	6.7	Recording and reporting

2.4 ISO standards terminology for risk management

There are key concepts conveyed by selected standards for the PhD thesis: ISO 31000, Annex SL, ISO 9001, ISO 21500, ISO/IEC 20000-1 and ISO/IEC 27001. In addition, there are associated standards which are dedicated to the concepts and terminology: these are ISO Guide 73, ISO 9000, ISO/IEC 20000-10, ISO/IEC 27000 and ISO/IEC 27005. The author is paying a particular attention to the ones provided by the ISO 31000 as the main reference, and checking shared used concepts and definitions in ISO Guide 73, Annex SL, ISO 9000, ISO 21500, ISO/IEC 20000-10 and ISO 27000. Moreover, there are summary tables of main definitions in chapter 6: this annex provides the definitions of all the discussed terms and show them in parallel, with the selected definition.

To start with, the author reminds 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 [101] defines Risk as the *“effect of uncertainty on an expected result”*. ISO/IEC 20000-10 [102] and ISO/IEC 27000 [103] 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. The author considers 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 [19]. **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*”. The author considers that the selected standards have a common meaning for the terms Context and Environment, but she favors 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. The author considers that the relevant definition of Communication and consultation for the PhD’s 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/IEC 20000-10 does not define Review but defines Monitoring as: “*determining the status of a system, a process or an activity*”. The author considers that the selected standards have a common meaning for the terms Monitoring and Review.

Regarding the overall risk management process, the author also precises 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*”.
- **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”*.

The terminology is not completely aligned between ISO Guide 73, ISO 31000 and ISO 21500 with differences related to the use of *“assess”*, *“analyse”* 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), the Risk management overall process is part of a global framework. Some general definitions related to governance and management are then of particular interest. It can be quoted that *“Leadership and commitment”* are found in ISO 31000, and also 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 they have common defined aspects. Another term to be tackled 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 MSSs are aligned with this definition, even if there are slight differences due to the targeted domain, for instance 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. The author quotes 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 reviewed in this section will be used as reference points in the rest of this PhD thesis.

3. Research approach according to Design Science

This research is based on Design Science principles. According to Denning, Design Science is a “*problem-solving paradigm and seeks to create innovations that define the ideas, practices, technical capabilities and products through which the analysis, design, implementation, management and use of Information Systems can be effectively and efficiently accomplished*” [104]. Design Science aims to “*create things that serve human purposes, and then to create new and innovative artefacts*” [105] such as constructs, models, methods, and instantiations. Each designed artefact is aiming at improving the environment and the way to measure this improvement is investigated. By applying Design Science principles, the author aims to guarantee the value chain linking research and technological activities.

Peffer et al. proposes a model describing the Design Science Research (DSR) method with a set of six activities in a nominal sequence [106]. These activities interact and are iteratively performed.

- 1 - Problem identification and motivation
- 2 - Definition of the objectives for a solution
- 3 - Design and development
- 4 - Demonstration
- 5 - Evaluation
- 6 - Communication

In the context of this PhD, the author has selected Design Science as the research method because of the aim of creating artefacts to be used in IT settings: a PRM and a PAM for Integrated risk management processes based on ISO standards, with interactions and iterations for improving the proposed solution related to the problem to be solved. In the overall context of the TIPA Framework, the creation of the IRMIS PRM and PAM is similar with the creation of previous process models artefacts and is relevant compared to other theories for building and testing these artefacts.

Research questions of this PhD thesis are distributed among the activities of this DSR process model. RQ1 (How to identify risk management activities throughout various selected ISO standards targeting management systems?) relates to activity 1: Problem identification and motivation, and to Activity 2: Definition of the objectives for a solution; RQ2 (How to drive integration for risk management activities in IT settings?) relates to activity 3: Design and development and activity 4: Demonstration; while RQ3 (How to improve risk management processes) relates to activity 5: Evaluation.

The next sub-sections detail these activities for the creation of the PRM and PAM artefacts with a particular emphasis on activity 3 which is the main contribution of this PhD thesis. As proposed in Peffer et al. [106], several research entry points are possible such as problem-centered initiation for activity 1, objective-centered solution for activity 2, design and development centered initiation for activity 3, and client/context initiated for activity 4. In the context of this PhD thesis, the research entry point is problem-

centered initiation, and corresponds to the activity 1 Problem identification and motivation described in the next paragraph.

3.1 Problem identification and motivation

DSR activity: This activity aims at defining the specific research problem and justifying the value of a solution. The problem definition will be used to develop an artefact that can provide a solution. In order to motivate the value of a solution, this activity includes knowledge of the state of the problem and the importance of its solution.

IRMIS PRM & PAM project activity: Companies are facing multiple certifications requirements and regulations which are critical for competitive advantage; Risk management plays a central part in this multiple frameworks landscape. In this context, business and market constraints have been identified via industry partners, and via their experience in process assessment and improvement. It has led to the motivation related to the use of ISO standards which are critical, not only for risk management, but also for management systems, information security management, IT service management and project management. The problems practitioners face in industry regarding risk management improvement are then manifold in the context of ISO standards in IT Organizations. This led to the main research question as previously mentioned: *“how to improve risk management processes in IT settings from an integrated and management system perspective in multiple ISO standards?”*.

3.2 Definition of the objectives for a solution

DSR activity: This activity aims at inferring the objectives of a solution from the problem definition and knowledge of what is possible and feasible.

IRMIS PRM & PAM project activity: In the PhD’s case, the targeted solution for managing risk and improving risk management with a process-based approach in IT settings is a PRM & PAM integrating risk management and based on ISO standards. The objectives for this solution are connected and limited to ISO standards, and the solution needs a structured, integrated, interoperable, assessable, effective and efficient way. Then, aligned with the problem to be solved and the available “material” provided by ISO standards, the selection of ISO standards was based on the choice of management systems and/or PDCA related relevant standards for the market within IT settings. Based on the state-of-the-art, the selected standards are: ISO 31000 as the main standard and international generic reference for risk management, and other standards such as the Annex SL for its HLS, ISO 9001, ISO/IEC 20000-1 and ISO/IEC 27001 for management system standards, and finally ISO 21500 for its process-orientation as well as PDCA structure. In terms of PRM and PAM, what is possible and feasible has to be aligned with the requirements of ISO/IEC 33004 (Requirements for process reference, process assessment and maturity models) [77] and to follow recommendations of the ISO/IEC 24774 (Guidelines for process description) [107]. When needed, mappings between versions of standards are provided; the latest version of each standard is used.

3.3 Design and development

DSR activity: This activity aims at creating the artefact(s). These artefacts can be “constructs, models, methods, or instantiations” or “new properties of technical, social, and/or informational resources”.

IRMIS PRM & PAM project activity: For creating the PRM & PAM, a Transformation process is applied, based on a GORE technique to provide guidance on how to transform a set of domain requirements into PRMs and PAMs which are compliant with the requirements of ISO/IEC 33004 and follow ISO/IEC TR 24774 guidance. The Transformation process advocates identifying elementary requirements and organising these requirements into requirement trees. These requirement trees are then oriented around the business goals to which they are related to form goal trees. The requirement and goal trees representation help PRM & PAM developers to visualize and support validation by experts. More details about this Transformation process can be found in [6]; the Transformation process has been applied successfully in various contexts and businesses [6, 7, 9, 12, 108]. The Transformation process is composed of nine steps. These steps are:

1. Identify elementary statements in a collection of requirements.
2. Organise and structure the requirements.
3. Identify common purposes upon those requirements and organise them towards domain goals.
4. Identify and factorise 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 the Outcomes.
9. Determine Work Products among the inputs and outputs of the practices.

This Transformation process is used iteratively in order to refine the grouping and process descriptions. Chapter 0 of the PhD thesis with the main research contribution provides details for each step when processes of the PRM and PAM are designed [C2, C3]. In the case of these works, the main ISO standard thread is the ISO 31000: this standard is not a management system one and does not provide requirements such as “shall” statements, but “should” statements. Each process is defined with the following characteristics mind-set: integration, assessability, interoperability, completeness, adoption and applicability. The process list of processes is displayed on Figure 1, and the process descriptions are available in Chapter 0 (Annex – IRMIS PAM).

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

Figure 1: IRMIS PAM proposed list of processes

3.4 Demonstration

DSR activity: This activity aims at demonstrating the use of the artefact to solve one or more instances of the problem. This can be done via the experimentation of the artefact's use.

IRMIS PRM & PAM project activity: This activity has been performed with a first loop of validation from a theoretical perspective with two experts with a practitioner background in process assessment (with ISO/IEC 15504-330xx expertise), management systems in IT organizations and project management including risk management. It enabled to show validation of the artefacts with domain expert reviews, in particular with risk management experts for the specific risk management processes. In a next DSR iteration, process assessment experimentations are expected in order to experiment the PAM's use and are planned after this PhD thesis with organizations that are currently looked for. A first experimentation could be performed in LIST according to the TIPA Framework [13] adapted to the IRMIS PAM with two types of risk domain: IT-related projects and information security (using the TIPA Framework with the TIPA method means interviewing people in companies). Managing projects is part of the day-to-day activities of researchers of the public research centre and an ISO/IEC 27001 certification is currently prepared for ensuring better information security practices. Another organization combining ISO 9001, ISO/IEC 20000-1 and ISO/IEC 27001 will be researched for if possible having a case study encompassing all targeted ISO standards of this PhD thesis. According to the targeted organization for the process assessment, several interviewees will have to be selected for several processes according to their role related to projects, IT services and information security: process operator, process manager, organizational and/or quality management responsible, risk management officer, risk manager. Beyond the PRM and PAM artefacts, the process assessment method may have to be adapted to the particular context of integrated risk management related to various ISO standards.

3.5 Evaluation

DSR activity: This activity aims at observing and measuring how well the artefact supports a solution to the problem. This activity involves comparing the objectives of a solution to actual observed results from use of the artefact in the demonstration. It requires knowledge of relevant metrics and analysis techniques.

IRMIS PRM & PAM project activity: The use of experts and peer reviewers to gain feedback on the artefacts and subsequent revisions of the artefacts show evaluation work. A careful observation and measurement of the artefacts has been performed from a qualitative perspective and was completed by two experts who reviewed the PRM and PAM with the evaluation grid below. More DSR iterations can be performed with experimentation throughout process assessment; the PRM and PAM can then be reviewed by users: assessors and interviewees of the process assessment (assessors have the process assessment background enabling to evaluate the PAM, both from the technical expertise in process assessment point of view and the domain expert one; interviewees have the domain expert point of view which can be whether from the organizational and quality practitioner point of view for management system processes, or from the operational point of view on risk management; for both views, officers and managers have to be interviewed), and can also evaluate criteria in the following grid.

Table 5: IRMIS PAM evaluation grid

	Disagree	Partially agree	Largely agree	Fully agree	No opinion	Comments
The number of processes is appropriate.						
The process names are meaningful.						
The overview of the PRM helps to understand the processes interactions.						
The PRM covers the statements of the ISO 31000:2018 standard from clauses 5 to clauses 6.						
The wording is clear and appropriate.						
The vocabulary used in this model is consistent.						
The Leadership process is appropriate						
The common processes are appropriate for management system mechanisms.						
The risk management specific processes are appropriate.						
The additional views provided in the PAM for project management and information security helps the PAM users to contextualize the type or risk.						

	Disagree	Partially agree	Largely agree	Fully agree	No opinion	Comments
A process assessment with the IRMIS PAM provides the means to improve risk management processes.						

For each process of specific risk management processes (risk management process group), all components have been reviewed in detail by the two experts mentioned in the Demonstration activity 4, and specific risk management processes were exposed in scientific communications (see in activity 6 of the DSR cycle); 15 peer reviewers provided some overall feedback on the PRM and the PAM, and some detailed feedback on the process descriptions of the specific risk management processes.

For management system specific processes (Leadership process group, Common processes group), a sound basis has been used from related works [9], and more particularly from ISO/IEC 33072 [52] and ISO/IEC 33073 [85] respective PAMs. These PAMs were submitted to the usual ISO ballots system, comments were provided by the various country members participating in the ISO/IEC JTC1 SC7 [17] for WG10 dedicated to process assessment and consensus was reached. It means that comments from experts worldwide had been made after several ballot rounds before the official public publication of these documents. The choices made by the author in terms of processes elicitation were exposed and reviewed via the various scientific communications (see in activity 6 of the DSR cycle), as for the specific risk management processes.

According to the evaluation grid, a SWOT analysis can determine Strengths, Weaknesses, Opportunities and Threats, and the IRMIS PRM and PAM can be updated accordingly.

3.6 Communication

DSR activity: This activity aims at communicating the problem and its importance, the artefact, its utility and novelty, the rigor of its design, and its effectiveness to researchers and other relevant audiences such as practicing professionals, when appropriate.

IRMIS PRM & PAM project activity: this PhD thesis is part of the communication as well as all papers supporting this research work [C1, C2, C3, C4, C7, C9]. The participation to ISO meetings and commenting similar artefacts also contributes to the confrontation of these works to experts and practitioners, as well as case studies for demonstrating and evaluating the PRM and PAM. In the future, the PRM and the PAM can be proposed by the author to the ISO community via the Luxembourg national body as a new work item proposal: researchers who participated to conferences with published papers [C4, C7, C9] and ISO experts already showed interest to the author for the PhD work results.

After describing the six activities of the DSR method of this PhD's research works, next chapter focuses on research contributions with the design and development of the main artefacts (IRMIS PRM and PAM) as the main contribution of the PhD thesis and components of the intermediary artefacts that can be found in annexes (as well as one of the main artefact: the IRMIS PAM):

- Chapter 6: terminology tables. Terms and concepts of various standards are presented in parallel, with ISO 31000 as the main reference; the selected terms are shown.
- Chapter 0: elementary statements from ISO 31000:2018. All statements of clauses 5 (Framework) and 6 (Process) are presented as elementary statements (each sentence is broken down as simplest as possible with a subject, a verb, and an order if any).
- Chapter 0: requirement trees and goal trees are presented for each specific risk management process (requirement trees represent the organisation of the elementary statements with logic grouping of concepts).
- Chapter 0: IRMIS PAM. The processes are described in terms of purpose, outcomes and base practices; work products and special views are provided for specific risk management processes.

4. Research Contributions

This chapter presents the main research contributions of this PhD thesis with three journal papers which represent the most significant performed work.

In order to address RQ1 “How to identify risk management activities throughout various selected ISO standards targeting management systems?”, a mapping of ISO 31000 with ISO selected standards has been performed and is presented in [C1]. The main principles with the PDCA approach were identified, including management system ones, process-based approach and risk-based thinking.

In order to address RQ2 “How to drive integration for risk management activities in IT settings?”, several intermediary artefacts have supported the progressive approach towards the main artefacts (IRMIS PRM and PAM):

- terminology has been studied in [C3] and terminology tables are providing a detailed view on definitions given in parallel for each term or set of terms (see chapter 6 with the Annex – Terminology tables);
- elementary statements have been identified from the ISO 31000 standard (see chapter 0: Annex – Elementary statements from ISO 31000:2018). From these elementary statements, some groupings were performed around common objects: a graphical view is provided in Requirements trees. Processes were then progressively identified and listed in a PRM process map according to the DSR method [C2] and the Transformation process [C2] for designing PRMs and PAMs as specified in Chapter 0. All the approach for determining processes is described in [C3], supported by the terminology study, the requirements trees and some mappings between standards for confirming some hypotheses.

In order to address RQ3 “How to improve risk management processes”, some intermediary artefacts were produced, as well as the major ones, the IRMIS PRM and PAM:

- then, identification and organization of common purposes was performed throughout goal trees (see chapter 0: Annex with requirements trees and goal trees for risk management specific processes). An example of Goal tree is provided in [C3].
- the IRMIS PRM and PAM was populated with management systems processes and risk management specific processes. Several examples of process descriptions are provided in [C2] and in [C3]. The IRMIS PAM is presented in Chapter 0 (Annex - IRMIS PAM).

4.1 Research contribution C1

- C1. Barafort, B.; Mesquida, A.L. & Mas, A. **Integrating risk management in IT settings from ISO standards and management systems perspectives**. *Computer Standards & Interfaces*, Volume 54, Part 3, November 2017, Pages 176-185.

4.1.1 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.

4.1.2 C1 Paper



Integrating risk management in IT settings from ISO standards and management systems perspectives



Béatrix Barafort^a, Antoni-Lluís Mesquida^{b,*}, Antonia Mas^b

^a Luxembourg Institute of Science and Technology, 5 Avenue des Hauts-Fourneaux, L-4362 Esch-sur-Alzette, Luxembourg

^b Department of Mathematics and Computer Science, University of the Balearic Islands, Ctra. de Valldemossa, km. 7.5, E07122 Palma de Mallorca, Spain

ARTICLE INFO

Keywords:

Risk management
Risk management process
Integrated risk management
Management system
Integrated management system
IT settings
ISO standards

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.

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

* Corresponding author.

E-mail addresses: beatrice.barafort@list.lu (B. Barafort), antoni.mesquida@uib.es (A.-L. Mesquida), antonia.mas@uib.es (A. Mas).

<http://dx.doi.org/10.1016/j.csi.2016.11.010>

Received 23 September 2016; Received in revised form 21 November 2016; Accepted 24 November 2016

Available online 30 November 2016

0920-5489/© 2016 Elsevier B.V. All rights reserved.

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 meta-model 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, 21] 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, 27,536 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 that 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 subsections 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:

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 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

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 management policy		0.3.3 Risk-based thinking 6.1 Actions to address risks and opportunities A.5 Applicability	3.4 Organizational strategy and projects	4.5.2 Plan the SMS (Plan)	5.2 Policy
			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	5.2 Plan new or changed services 6.6.1 Information security 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 3.6 Project Governance 4.3.40 Manage communications 4.3.40 Manage communications		
4.3.6 Establishing internal communication and reporting mechanisms					
4.3.7 Establishing external communication and reporting mechanisms					
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 Communication and consultation		4.2 Understanding the needs and expectations of interested parties 4.1 Understanding the organization and its context	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				
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)

(continued on next page)

Table 2 (continued)

	ANNEX SL	ISO 9001:2015	ISO 21500:2012	ISO/IEC 20000-1:2011	ISO/IEC 27001:2013
5.4.2 Risk identification	6.1 Actions to address risks and opportunities	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 opportunities	6.1 Actions to address risks and opportunities (6.1.2)	4.3.30 Treat risks		6.1.3 Information security risk treatment
5.5.3 Preparing and implementing risk treatment plans	6.1 Actions to address risks and opportunities	6.1 Actions to address risks and opportunities			6.2. Information security objectives and plans to achieve them
5.6 Monitoring and review		9.1.3 Analysis and evaluation 9.3.2 Management review inputs 10.2 Nonconformity and corrective action	4.3.31 Control risks		8.3 Information security risk treatment
					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 4.2 in ISO 31000)
- Leadership and commitment (Section 4.3 in ISO 31000)
- Plan-Do-Check-Act (PDCA) cycle (Section 4.3.4 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

4.3.3.1. 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”.

4.3.3.2. 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 Fig. 1 and comprises the activities described in ISO 31000 clauses 5.2–5.6.

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.

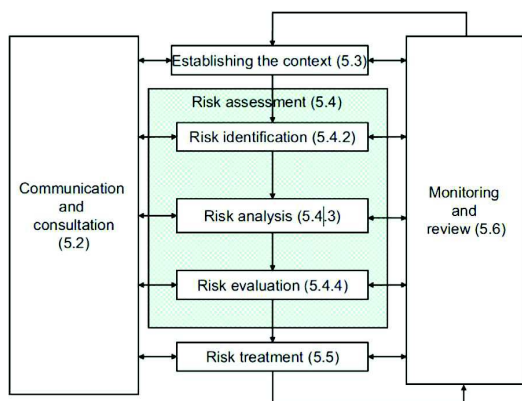


Fig. 1. ISO 31000 Risk management process.

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*”.

4.3.3.3. . *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).

4.3.3.4. *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.

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

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

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.

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] S. Cots, M. Casadesús, Exploring the service management standard ISO 20000, *Total Qual. Manage. Bus. Excell.* 26 (5–6) (2015) 515–533 (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] B. Henderson-Sellers, C. Gonzalez-Perez, T. McBride, G. Low, An ontology for ISO software engineering standards: 1) creating the infrastructure, *Comput. Stand. Interfaces* 36 (3) (2014) 563–576.
- [15] X. Larrucea, C. Gonzalez-Perez, T. McBride, B. Henderson-Sellers, Standards-based metamodel for the management of goals, risks and evidences in critical systems development, *Comput. Stand. Interfaces* 48 (2016) 71–79.
- [16] S. Jeners, P. Clarke, R.V. O'Connor, L. Buglione, M. Lepmets, Harmonizing software development processes with software development settings—a systematic approach, in: *Proceedings of the European Conference on Software Process Improvement*, Springer Berlin Heidelberg, 2013, pp. 167–178.
- [17] X. Larrucea, I. Santamaría, An industrial assessment for a multimodel framework, *J. Softw.: Evol. Process* 26 (9) (2014) 837–845.
- [18] X. Larrucea, I. Santamaría, R. Colomo-Palacios, Assessing ISO/IEC29110 by means of ITMark: results from an experience factory, *J. Softw.: Evol. Process* (2016).
- [19] M.T. Baldassarre, D. Caivano, F.J. Pino, M. Piattini, G. Visaggio, Harmonization of ISO/IEC 9001: 2000 and CMMI-DEV: from a theoretical comparison to a real case application, *Softw. Qual. J.* 20 (2) (2012) 309–335.
- [20] C. Pardo, F.J. Pino, F. García, M. Piattini, M.T. Baldassarre, An ontology for the harmonization of multiple standards and models, *Comput. Stand. Interfaces* 34 (1) (2012) 48–59.
- [21] C. Pardo, F.J. Pino, F. García, M.T. Baldassarre, M. Piattini, From chaos to the systematic harmonization of multiple reference models: a harmonization framework applied in two case studies, *J. Syst. Softw.* 86 (1) (2013) 125–143.
- [22] C.J. Pardo-Calvache, F.O. García-Rubio, M.G. Piattini-Velthuis, F.J. Pino-Correa, M.T. Baldassarre, A 360-degree process improvement approach based on multiple models, *Rev. Fac. Ing. Univ. Antioq.* 77 (2015) 95–104.
- [23] M. Casadesús, S. Karapetrovic, I. Heras, Synergies in standardized management systems: Some empirical evidence, *TQM J.*, 23(1), Emerald Insight, 2011, pp. 73–86.
- [24] A. Simon, S. Karapetrovic, M. Casadesús, Difficulties and benefits of integrated management systems, *Ind. Manage. Data Syst.*, 112(5), Emerald Insight, 2012, pp. 828–846.
- [25] A.L. Mesquida, A. Mas, Integrating IT service management requirements into the organizational management system, *Comput. Stand. Interfaces*, 37, Elsevier, 2015, pp. 80–91.
- [26] A.L. Mesquida, A. Mas, E. Amengual, I. Cabestrero, 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), ATI, 2010, pp. 25–34.
- [27] A. Mesquida, A. Mas, T. San Feliu, M. Arcilla, MIN-ITs: a framework for the integration of IT management standards in mature environments, *Int. J. Softw.* 24 (06) (2014) 887–908 (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] F. Mc Caffery, J. Burton, I. Richardson, Risk management capability model for the development of medical device software, *Softw. Qual. J.* 18 (2010) 81. <http://dx.doi.org/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] P. Domingues, P. Sampaio, P.M. Arezes, Integrated management systems assessment: a maturity model proposal, *J. Cleaner Prod.* (2016). <http://dx.doi.org/10.1016/j.jclepro.2016.02.103>.
- [34] B. Barafort, A. Renault, M. Picard, S. Cortina, A transformation process for building PRMs and PAMs based on a collection of requirements – example with ISO/IEC 20000. In: A. Dorling, T. Rout, R. Treffny (Eds.), *SPICE 2008*, Global Association for Software Quality, Nuremberg, 2008.
- [35] S. Cortina, N. Mayer, A. Renault, B. Barafort, Towards a process assessment model for management system standards. In: A. Mitasianas, T. Rout, R.V. O'Connor, A. Dorling, (Eds.) *SPICE 2014*, CCIS, vol. 477, Springer, Heidelberg, 2014, pp. 36–47.
- [36] ISO/IEC 27005: Information Technology – Security Techniques – Information Security Risk Management – Requirements, International Organization for Standardization, Geneva, 2011.
- [37] A.S.O. Parra, L.E.S. Crespo, E. Alvarez, M. Huerta, E.F.M. Paton, Methodology for dynamic analysis and risk management on ISO27001, *IEEE Lat. Am. Trans.* 14 (6) (2016) 2897–2911.
- [38] D.C. Chou, Cloud computing risk and audit issues, *Comput. Stand. Interfaces* 42 (2015) 137–142.
- [39] A.-L. Mesquida, A. Mas, M. Lepmets, A. Renault, Development of the project management SPICE (PMSPICE) framework. in: A. Mitasianas, T. Rout, R.V. O'Connor, A. Dorling, (Eds.) *SPICE 2014*, CCIS, vol. 477, Springer, Heidelberg, 2014, pp. 60–71.
- [40] A.-L. Mesquida, A. Mas, B. Barafort, The project management SPICE (PMSPICE) process reference model: towards a process assessment model. in: R.V. O'Connor, et al. (Eds.) *EuroSPI 2015*, CCIS, vol. 543, Springer, Heidelberg, 2015, pp. 193–205. (http://dx.doi.org/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 No. 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] A. Guide, Project management body of knowledge (PMBOK® GUIDE), Project Manag. Inst. (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.

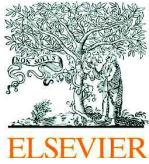
4.2 Research contribution C2

- C2. Barafort, B.; Mesquida, A.L. & Mas, A. **Integrated Risk Management Process Assessment Model for IT Organizations based on ISO 31000 in an ISO Multi-Standards Context.** *Computer Standards & Interfaces*, In Press, Corrected Proof, 2018.

4.2.1 Abstract

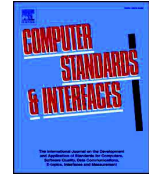
With risk management as a key challenge for most organizations, aligning and improving organisational and business processes is essential. Capability and Maturity Models can contribute to assess and then enable process improvement. With the need to integrate risk management in IT Organizations (IT department/organisation), ISO/IEC 15,504–330xx process assessment approach combined with the latest version of ISO 31,000 for risk management can be the foundations for new process models. An integrated process-based approach with various popular and market demands ISO standards (ISO 9001, ISO 21,500, ISO/IEC 20,000–1 and ISO/IEC 27,001) is proposed in the paper; it explains how the Integrated Risk Management Process Assessment Model for IT Organizations in an ISO multi-standards context is developed with a Design Science research method.

4.2.2 C2 Paper



Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context

Béatrix Barafort^{a,*}, Antoni-Lluís Mesquida^b, Antònia Mas^b^a Luxembourg Institute of Science and Technology, 5 Avenue des Hauts-Fourneaux, L-4362 Esch-sur-Alzette, Luxembourg^b University of the Balearic Islands, Department of Mathematics and Computer Science, Cra. De Valldemossa, km 7.5, Palma de Mallorca, Spain

ARTICLE INFO

Keywords:

Integrated risk management
IT organizations
ISO/IEC 15504–330xx
Process reference and assessment models
engineering
Design science research method

ABSTRACT

With risk management as a key challenge for most organizations, aligning and improving organisational and business processes is essential. Capability and Maturity Models can contribute to assess and then enable process improvement. With the need to integrate risk management in IT Organizations (IT department/organisation), ISO/IEC 15,504–330xx process assessment approach combined with the latest version of ISO 31,000 for risk management can be the foundations for new process models. An integrated process-based approach with various popular and market demands ISO standards (ISO 9001, ISO 21,500, ISO/IEC 20,000–1 and ISO/IEC 27,001) is proposed in the paper; it explains how the Integrated Risk Management Process Assessment Model for IT Organizations in an ISO multi-standards context is developed with a Design Science research method.

1. Introduction

Nowadays, risk management is a key challenge for most of the organizations. Qualitative and quantitative approaches of risk management can be deployed. Capability & Maturity Models (C&MM) contribute to the Risk management practitioners by providing instruments for measuring process capability during process assessment and enabling improvement. Organizations wishing to improve risk management face the problematic of choosing and selecting the right approach aligned to their business challenges and market positioning. Related to the area of C&MM, the International Standardization Organization (ISO) have published at the beginning of the years 2000 the international standard series on Process assessment (ISO/IEC 15504 [1]), now revised and published in the ISO/IEC 330xx standard series [2]. The main normative documents of the series provide requirements for a structured and systematic approach for process assessment (for capability process assessment and/or organizational maturity), process reference and process assessment models description, and some guidance related to process assessment and improvement. ISO standard series for Process assessment (PA) provides a consensus and was the basis for various initiatives proposing Process Models structured on the way enabling ISO/IEC 330xx compliant PA on the one hand at ISO level [3–9], and on the other hand at market level [10–13]. Among these various ISO/IEC 15504–330xx process models, none is dedicated to risk management, even if risk management is addressed in most of them on a broad way. On top of that, in many IT organizations, management

systems are mandated by the market in terms of certifications such as ISO/IEC 27001 [14] for information security management, ISO/IEC 20000–1 [15] for IT service management and ISO 9001 [16] for quality management. Project management remains a key concern for IT Organizations; the project management standard ISO 21500 [17] relies on a management system for mastering projects, including managing project risks. According to industry feedback and author experiences, these topics (quality management, project management, information security management and IT service management) are the most commonly addressed by many IT organizations, whatever their size and domain; we have selected them for being part of our research in a PA context. When we study these various topics, the nature of the managed risks varies, but the mechanisms of the practices for managing risks are not varying in a management system environment. This is a key point to consider.

We had investigated *how to integrate risk management in IT Organizations within a management system context?* in previous works [18]. By IT Organizations, we mean any IT department or IT company needing to integrate risk management activities. The authors made the assumption that an integrated risk management approach for IT Organizations will benefit organizations by being based on ISO standards which represent international consensus. Our assumption is supported by market demand for ISO 9001, ISO/IEC 27001 and ISO 20000–1 as popular standards for certification of management systems, completed by ISO 21500 because project management is always a critical process in IT organizations. So these standards are the ground material of our

* Corresponding author.

E-mail addresses: beatrice.barafort@list.lu (B. Barafort), antoni.mesquida@uib.es (A.-L. Mesquida), antonia.mas@uib.es (A. Mas).<https://doi.org/10.1016/j.csi.2018.04.010>Received 8 February 2018; Received in revised form 23 April 2018; Accepted 29 April 2018
Available online 10 May 2018

0920-5489/ © 2018 Elsevier B.V. All rights reserved.

research. With this background, our current research is investigating the following research question: *how to improve risk management processes in IT Organizations from a management system perspective?* For doing so, some more previous works have already justified the need to identify processes for a new Integrated Risk Management process model for IT Organizations (IRMIS) [19,20] based on the ISO 31000 standard for Risk management [21,22]. It is the international reference in the domain. With ISO 31000 as our guideline, the integration is considered regarding ISO 9001, ISO 21500, ISO/IEC 20000–1, and ISO/IEC 27001. Since ISO standards are always subject to review and revision when relevant, we consider some versions of standards which are about to be published, in order to be as aligned as possible with the state of the art in the ISO community, and to leverage competitive advantage on the market. As ISO 31000 is under revision at ISO level, with an imminent new version to be published, our research works are taking into account the Final Draft International Standard (FDIS) [22] prepared at the end of 2017 (last step before publication). In the same vein, we consider the Draft International Standard of ISO/IEC 20000–1 (antepenultimate version before publication). By taking into account these latest versions, some updates are provided considering the IRMIS PAM list of processes and their description.

According to our research question, we aim at supporting Risk management processes improvement in IT Organizations, with a structured, integrated, interoperable, assessable, effective and efficient way via a PRM and a PAM as artefacts enabling process assessment and improvement. These two artefacts extend the ISO 31000 standard which is already process-oriented, but not structured neither organised for rigorous process assessment, neither specifically addressing IT Organizations. So this paper presents the first results achieved with the development of a PRM and a PAM for IRMIS, implementing a Transformation process [23] supporting the design of process models according to ISO/IEC 15504/330xx. In order to develop these artefacts, a Design Science Research Method [24] is followed.

Section 2 presents Related work and ISO standards inputs, and Section 3 introduces the Design Science Research Method. Section 4 presents the PAM development of the core risk management processes with views on the other ISO standards targeted in the IT Organizations scope of our research; this development has followed the Transformation process applied to ISO 31000 and a first loop of rigorous validation. Finally, Section 5 concludes the paper and presents future research perspectives.

2. Related work and ISO standards inputs

A lot of work has targeted Risk management in various domains. Capability & Maturity Models (C&MM) are amongst them. A recent paper presenting the LEGO approach (Living EnGineering pROcess: approach to process improvement) to achieve a meta-model on Risk Management merging various sources, includes a survey on Risk management C&MM which has shown and compared their respective approaches [25]. They were different in structure and levels. To ensure integration and consistency, and to align with market demands and pressures related to certifications, our research focuses on PRMs and PAMs fulfilling ISO/IEC 15504/330xx requirements on Process assessment and encompassing management systems principles. The economic benefits of standards is demonstrated in the industry [26], in particular with ISO certifications such as the most popular one: ISO 9001 [16] which is mentioned in the annual ISO survey on certifications of management systems standards [27].

We have studied existing and available PRMs & PAMs related to Risk management in C&MM context, based on publicly available ISO/IEC 15504/330xx. Table 1 lists these Risk management processes and their source.

According to these processes, the risk management process, as addressed by the ISO 31000 standard, is very general. There is little difference among these processes, where risk identification is performed,

and then analysis and evaluation, from the risk assessment perspective, and finally risk treatment. There is not much detail in each of these PAM. As illustration, you can see below in Table 2, extracted from the latest published standard ISO/IEC 33073 Process Capability Assessment Model [8], the Risk management process description:

In addition to Table 1, some closely related works have been performed in the medical IT networks domain with a PRM and PAM for improving risk management, in order to allow Healthcare Delivery Organisations to assess the capability of their risk management processes against the requirements of IEC 80000–1 (application of risk management to IT-networks incorporating medical devices) [28]. There are 14 processes for different aspects of the life cycle risk management. In this process model, there are 4 processes dedicated to the risk management itself: Medical IT Network Risk Management, Risk Analysis & Evaluation, Risk Control, and Residual Risk. This approach is targeting the medical sector with a particular objective of contribution to ISO 80000–1 but with a common overall goal with our works for improving risk management processes. We nevertheless address management systems from various selected ISO standards perspectives in an IT Organizations mind-set, as indicated in the next paragraph.

Some recent works have directly addressed the ISO 31000 standard for risk management in order to propose a Maturity Model for risk management [29]. The paper analyses existing Risk management related maturity models and selects some inputs, for instance in CMMI for its structure. Then it proposes a new maturity model. This maturity model does not fulfil the ISO/IEC 330xx requirements for process capability and maturity assessment.

In previous works, the authors explored risk management in IT Organizations from the perspective of relevant ISO standards driven by market demand and authors expertise (targeting quality management, project management, IT service management and information security management), with ISO 31000 as main theme. Table 3 provides the full list with identification numbers and titles of each considered standard, with an additional standard bringing valuable insights on information security risk management: ISO/IEC 27005 [30]. For quality management, the ISO 9001 standard specifies that “*there is no requirement for formal methods for risk management or a documented risk management process. Organizations can decide whether or not to develop a more extensive risk management methodology than is required by this International Standard, e.g. through the application of other guidance or standards.*” The ISO/IEC 20000–1 standard is in the same vein. The current standards highlight the role of Risk management but do not offer comprehensive pathways.

It is also relevant to highlight that there is an important aspect in implementing standards: its version. Standards are continuously revised, when relevant. There is an official standard lifecycle at ISO, and once published, there is a systematic review every five years. As stated on ISO web site, “*Systematic Review provides valuable information on the global relevance of the standard and ensures that the ISO catalogue is up-to-date. It is also currently the only systematic way for the ISO Central Secretariat to collect information on the use of ISO standards and their national adoption.*” In Table 1, two listed standards are not in their final published version: the ISO 31000, in Final Draft International Standard phase (FDIS), and ISO/IEC 20000–1 in Draft International Standard phase (DIS). As the ISO 31000 is the main driver of our work, we decided to adopt the latest version because the final publication will be nearly identical to the FDIS document. We checked the alignment of clauses in Table 3.

In Table 4 is the list of relevant standards considered in our works, supporting the development of a PRM and a PAM for Integrated Risk Management in IT Organizations.

In previous works, the authors had shown that management system standards (MSS) mechanisms are present in standards listed in Table 4 (ISO 9001, ISO 20000–1, and ISO/IEC 27001, as well as ISO 21500, even if it is not a requirements standard enabling a management system certification. These mechanisms help integrating processes, and

Table 1
List of Risk management processes in existing Process models fulfilling ISO/IEC 15504-330xx requirements for PRM & PAM.

Process model	Name of the Risk management related process(es)
ISO/IEC 15504-5:2012 – Part 5: An exemplar software life cycle process assessment model [3]	MAN.5 Risk management
ISO/IEC 15504-6:2013 – Part 6: An exemplar system life cycle process assessment model [4]	PRJ.5 Risk management
ISO/IEC 15504-8:2012 – Part 8: An exemplar process assessment model for IT service management [5]	SMS.6 Risk management
Enterprise SPICE (ISO/IEC 33071:2016 – An integrated process capability assessment model for Enterprise processes) [6]	GVM.9 Risk management
ISO/IEC 33072:2016 – Process capability assessment model for information security management [7]	COM.11 Risk and opportunity management
ISO/IEC 33073:2017 – Process capability assessment model for quality management [8]	COM.11 Risk management
ISO/IEC 30105-2: 2016 – Information technology – IT Enabled Services-Business Process Outsourcing (ITES-BPO) lifecycle processes – Part 2: Process assessment model (PAM) [9]	ENB1 Risk management
Automotive SPICE Process Assessment Model [10]	MAN.5 Risk management
COBIT Process Assessment Model (PAM): Using COBIT 5 [11]	EDM03 Ensure risk optimisation Manage risk

Table 2
Extract from ISO/IEC 33073: the Risk management process description.

Process ID	COM.11
Name	Risk management
Purpose	The purpose of Risk Management is to identify, analyse, evaluate, treat and monitor risks.
Outcomes	As a result of successful implementation of this process: 1. Risks are identified. 2. Identified risks are analysed. 3. Risks are evaluated against defined criteria. 4. Risks are selected for treatment. 5. Selected risks are treated.

Table 4
List of relevant ISO standards supporting IRMIS PRM and PAM.

ISO Standard number	ISO Standard title
ISO FDIS 31000:2017 [22]	Principles and generic guidelines on risk management
ISO 9001:2015 [16]	Quality management systems - Requirements
ISO 21500:2012 [17]	Guidance on project management
ISO/IEC DIS 20000-1:2017 [15]	Information Technology - Service management - Part 1: Service management systems requirements
ISO/IEC 27001:2013 [14]	Information Technology - Security techniques - Information security management systems - Requirements
ISO/IEC 27005:2011 [30]	Information Technology - Security techniques - Information security risk management

proposing common core processes as well as risk management dedicated processes, in a single model addressing mechanisms for several types of risks related to project, process, information security, and IT services.

3. Research method

This research is based on Design Science principles. According to Denning, Design science is a “*problem-solving paradigm and seeks to create innovations that define the ideas, practices, technical capabilities and products through which the analysis, design, implementation, management*

and use of Information Systems can be effectively and efficiently accomplished” [31]. Design Science aims to “*create things that serve human purposes, and then to create new and innovative artefacts*” [32] such as constructs, models, methods, and instantiations. Each designed artefact is aiming at improving the environment and the way to measure this improvement is investigated. By applying design science principles, we aim to guarantee the value chain linking research and technological activities.

Peffer et al. proposes a model describing the Design Science Research Method (DSRM) with a set of six activities in a nominal

Table 3
Mapping of clauses between ISO 31000:2009 and ISO 31000:2017 (FDIS).

ISO 31000:2009	ISO 31000:2017		
4.2	Mandate and commitment	5.2	Leadership and commitment
4.3.1	Understanding of the organization and its context	5.3.1	Understanding of the organization and its context
4.3.2	Establishing risk management policy	5.3.2	Articulating risk management commitment
4.3.3	Accountability	5.3.3	Assigning organizational roles, authorities, responsibilities and accountabilities
4.3.4	Integration into organizational processes	5.2.2	Integrating risk management
4.3.5	Resources	5.3.4	Allocating resources
4.3.6	Establishing internal communication and reporting mechanisms	5.3.5	Establishing communication and consultation
4.3.7	Establishing external communication and reporting mechanisms	5.3.5	
4.4.1	Implementing the framework for managing risk	5.4	Implementation
4.6	Continual improvement of the framework	5.5	Evaluation (NEW)
5.1	General	5.6	Improvement
5.2	Communication and consultation	6.1	General
5.3.2	Establishing the external context	6.2	Communication and consultation
5.3.3	Establishing the internal context	6.3.1	Establishing the context - General
5.3.4	Establishing the context of the risk management process	6.3.2	Establishing the context - Defining the purpose and scope
5.3.5	Defining risk criteria	6.3.3	Establishing the context - Context
5.4.2	Risk identification	6.3.4	Defining risk criteria
5.4.3	Risk analysis	6.4.2	Risk identification
5.4.4	Risk evaluation	6.4.3	Risk analysis
5.5.1	General - Risk Treatment	6.4.4	Risk evaluation
5.5.2	Selection of risk treatment options	6.5	Risk treatment
5.5.3	Preparing and implementing risk treatment plans	6.5.2	Selection of risk treatment options
5.6	Monitoring and review	6.5.3	Preparing and implementing risk treatment plans
5.7	Recording the risk management process	6.6	Monitoring and review
		6.7	Recording and reporting

sequence [24]. These activities interact and are iteratively performed. The next sub-sections details these design activities for the creation of the PRM and PAM artefacts with a particular emphasis on step 3 which is the main contribution of this paper (steps 1 and 2 have been reported in previous works [18]). Steps 4 and 6 are under progress while step 5 is planned in a near future.

3.1. Problem identification and motivation

DSR activity: This activity aims at defining the specific research problem and justifying the value of a solution. The problem definition will be used to develop an artefact that can provide a solution. In order to motivate the value of a solution, this set of activities includes knowledge of the state of the problem and the importance of its solution.

IRMIS PRM & PAM project activity: Companies are facing multiple certifications requirements and regulations which are critical for competitive advantage; Risk management plays a central part in this multiple frameworks landscape. In this context, business and market constraints have been identified via industry partners, and via their experience in process assessment and improvement. It has led to the motivation related to the use of ISO standards which are critical, not only for risk management, but also for management systems, information security management, IT service management and project management. The problems practitioners face in industry regarding risk management improvement are then manifold in the context of ISO standards in IT Organizations.

3.2. Define the objectives for a solution

DSR activity: This activity aims at inferring the objectives of a solution from the problem definition and knowledge of what is possible and feasible.

IRMIS PRM & PAM project activity: In our case, the targeted solution for managing risk and improving risk management with a process-based approach in IT Organizations is a PRM & PAM integrating risk management and based on ISO standards. The objectives for this solution are connected and limited to ISO standards, and the solution need a structured, integrated, interoperable, assessable, effective and efficient way. What is possible and feasible has to be aligned with the requirements of ISO/IEC 33004 (Requirements for process reference, process assessment and maturity models) and to follow recommendations of the ISO/IEC 24774 (Guidelines for process description) [33]. As much as possible, the latest version of each standard is used.

3.3. Design and development

DSR activity: This activity aims at creating the artefact(s). These artefacts can be “constructs, models, methods, or instantiations” or “new properties of technical, social, and/or informational resources”.

IRMIS PRM & PAM project activity: For creating the PRM & PAM, a Transformation process is applied, based on a goal oriented requirements engineering (GORE) technique to provide guidance on how to transform a set of domain requirements into PRMs and PAMs which are compliant with the requirements of ISO/IEC 33004 and follow ISO/IEC TR 24774 guidance. The Transformation process advocates identifying elementary requirements and organising these requirements into requirement trees. These requirement trees are then oriented around the business goals to which they are related to form goal trees. The requirement and goal trees representation help PRM & PAM developers to visualize and support validation by experts. More details about this Transformation process can be found in [23]. The Transformation process is composed of nine steps. These steps are:

1. Identify elementary statements in a collection of requirements.
2. Organise and structure the requirements.

3. Identify common purposes upon those requirements and organise them towards domain goals.
4. Identify and factorise 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 the Outcomes.
9. Determine Work Products among the inputs and outputs of the practices.

This Transformation process is used iteratively in order to refine the grouping and process descriptions. Section 4 of the paper provides details for each step. In the case of these works, we use the term “statement” instead of “requirements”, because our main ISO standard thread is the ISO 31000: this standard is not a management system one and does not provide requirements such as “shall” statements, but “should” statements.

3.4. Demonstration

DSR activity: This activity aims at demonstrating the use of the artefact to solve one or more instances of the problem. This can be done via the experimentation of the artefact’s use.

IRMIS PRM & PAM project activity: This activity has been initiated with a first loop of validation with expert with a background in process assessment, management systems in IT Organizations and project management including risk management; validation of the artefact is foreseen with more expert domain reviews and process assessment experimentations.

3.5. Demonstration

DSR activity: This activity aims at observing and measuring how well the artefact supports a solution to the problem. This activity involves comparing the objectives of a solution to actual observed results from use of the artefact in the demonstration. It requires knowledge of relevant metrics and analysis techniques.

IRMIS PRM & PAM project activity: Following experimentation(s) of the artefact, a careful observation and measurement of the experimentation will be performed (it is planned after the setting of metrics and selection of appropriate analysis techniques).

3.6. Communication

DSR activity: This activity aims at communicating the problem and its importance, the artefact, its utility and novelty, the rigor of its design, and its effectiveness to researchers and other relevant audiences such as practicing professionals, when appropriate.

IRMIS PRM & PAM project activity: this current paper is part of the communication as well as all papers supporting this research work [18–20]. The participation to ISO meetings and commenting similar artefacts also contributes to the confrontation of these works to practitioners.

After describing the six activities of the DSRM of our research works, next section will focus on the design and development of the artefacts.

4. Design and development of a PRM and a PAM for an integrated risk management process model dedicated to IT organizations

According to the Transformation process mentioned in Section 3, the PRM and PAM development has been performed. The first three steps have already been presented in [19]; they are summarized here in order to provide a full view of the approach but more specifically to

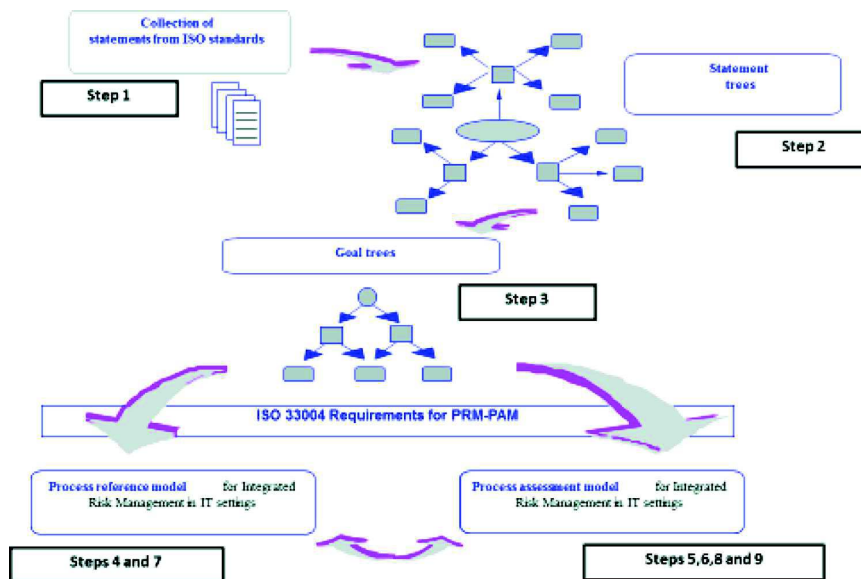


Fig. 1. Transformation process activities (adapted from [23]).

provide updates entailed by the new version of ISO 31000. We also quote that we aim at satisfying a set of criteria for the produced PRM and PAM, as stated in [23]. They will have to satisfy the following characteristics: assessability, interoperability, integration, completeness, adoption and applicability. Fig. 1 provides an overview of the Transformation process, with the positioning of the various steps.

The ISO 31000 standard is the main thread for the Transformation process. Other standards are considered in a second time, once the structure of each identified process is determined. Our assumption is that the PAM is contextualised to each targeted domain in an IT setting; project management (ISO 21500) and information security management (ISO/IEC 27001) provide, in particular, specific information that can be presented while ISO 9001 and ISO/IEC 20000–1 remain quite generic for respectively process quality and IT services. As already mentioned, the nature of the managed risks varies, but not the mechanisms of the practices for managing risks, particularly in a management system environment. So these mechanisms can be reused and applied to the various targeted domains.

Step 1: Identify elementary statements in a collection of statements

The first step of the Transformation process consists in identifying all of the statements to form a collection of elementary statements. ISO 31000 provides, for each clause, a set of statements which are formulated mainly with “should” statements, also with “may”, “can” or just information without any particular semantics format. The verbs in passive voice statements (revealing statements) were easily identified and split into elementary statements. Other sentences with a verb in present tense, clearly indicating an action to perform or a condition to be satisfied, were also considered elementary statements. When a sentence was composed of two parts separated by the coordination conjunction “and”, it was divided into two elementary statements. If there was an enumeration, each element of the list was identified as an elementary statement. Because the latest version of ISO 31000 has been considered recently, all work of identification of elementary statements has been redone with the latest collection of statements present in the ISO FDIS 31000:2017 [22].

Step 2: Organize, and structure the statements

During the second step, the elementary requirements were organized and gathered around the objects they are about in order to build a “statement tree” by applying mind mapping techniques. The

elementary “should statements” were organized, as well as relevant statements bringing valuable information, and structured under the form of a “mind map” for statement trees. This “mind map” helped to generate a graphical view of the elementary items having the same object (or component). A decision was made to distribute the set of statements in various statement trees; 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. This statement tree structuring was inspired by previous works where some groupings were similar.

Step 3: Identify common purposes upon those statements and organize them towards domain goals

From the statements tree, some common purposes were identified and the elementary statements were organized accordingly, taking the original meaning of the ISO 31000 statements into account. A goal tree was then built for each common purpose, in which the inter-related activities were properly grouped. At this stage, we were able to identify processes, at least for a first proposal of a process list which we are regularly refining, according to the various iterations that are possible all along the Transformation process and in the Design Science Research mind-set. Common processes were identified from the management system mechanisms (see Table 5). Risk management dedicated processes were identified from the Risk management process clauses with the associated domain goals revealed in goal trees: Risk criteria definition, Risk identification, Risk analysis and Risk evaluation, and then Risk Treatment and Recording and reporting. Sub-clauses in ISO 31000 guided these risk management dedicated processes. Considering the last version of ISO 31000, we checked the alignment of clauses and other management system standards PRM and PAM aligned with our works in order to propose an updated set of processes. The following mapping table shows this check and the updates taking into account the new version of ISO 31000 and the most recently published ISO PAM based on a Management System Standard: namely the ISO/IEC 33073 Process capability assessment model for quality management [8].

At this stage of our research work, we identified 6 processes for the Risk management process group. From a process assessment and risk management domain practitioner point of view, this may be reviewed at the validation phase with risk management domain experts, with aggregation in two or even one single process for Risk Assessment including Risk identification, Risk analysis and Risk evaluation, for

Table 5
Elicited list of processes deduced from ISO 31000 statements and various PAMs.

31000 Sub-clause	31000:2017 Sub-clause title	IRMIS PAM proposed processes	ISO/IEC 33073 (PAM 9001)	ISO 21500 Process subjects/groups
5.2	Leadership and commitment	TOP.01 Leadership	TOP.1 Leadership	
5.3.1	Understanding the organization and its context			
5.3.2	Articulating risk management commitment			
5.3.3	Assigning organizational roles, authorities, responsibilities and accountabilities			
6.3	Establishing the context			
6.3.4	Defining risk criteria	RIS.01 Risk criteria definition		
6.2	Communication and consultation	COM.01 Communication management	COM.01 Communication management	
	<i>Notions of documents</i>	COM.02 Documentation management	COM.02 Documentation Management	
5.3.4	Allocating resources	COM.03 Resource management	COM.03 Human resource management	Resource: 4.3.15 Establish project team; 4.3.16 Estimate resources 4.3.17 Define project organization; 4.3.18 Develop project team; 4.3.19 Control resources 4.3.20 Manage project team
5.6	Improvement	COM.04 Improvement	COM.04 Improvement	
	<i>No “audit” notion in 31000</i>	COM.05 Audit	COM.05 Internal audit	
6.6	Monitoring and review	COM.11 Monitoring	COM.06 Management review	
	<i>No “non-conformity” notion in 31000</i>	COM.06 Review		
		COM.07 Non-conformity management	COM.07 Non-conformity management	
		COM.08	COM.08	
5.4	Implementation	Operational planning COM.09	Operational planning COM.09	
		Operational Implementation and control	Operational implementation and control	
5.5	Evaluation	COM.10	COM.10	
		Performance evaluation	Performance evaluation	
6.4.2	Risk identification	RIS.02 Risk identification	COM.11 Risk management	Risk: 4.3.28 Identify risks 4.3.29 Assess risks 4.3.30 Treat risks 4.3.31 Control risks
6.4.3	Risk analysis	RIS.03 Risk analysis		
6.4.4	Risk evaluation	RIS.04 Risk evaluation		
6.5.1	General - Risk Treatment	RIS.05 Risk Treatment		
6.5.2	Selection of risk treatment options			
6.5.3	Preparing and implementing risk treatment plans			
6.7	Recording and reporting	RIS.06 Reporting and recording	COM.02 Documentation Management	

usability, efficiency and assessability reasons. The PRM list of elicited processes is available in Fig. 2. Because Annex SL was driving the management system aspects of ISO 31000 (even if it is not prescriptive in our case, the structure of core common processes has been kept. Because some processes are not necessary in the case of ISO 31000 transposition into a PRM, but in an integration mindset, these processes appear in the process list in italic (COM.05 Internal audit, and COM.07 Non-conformity management). A validation loop has been performed at this stage in order to review that: the number of processes is appropriate; the process names are meaningful; the overview of the PRM helps to understand the process interactions; the PRM covers the statements of the ISO 31000:2017 standard from clauses 5 and clauses 6. This validation loop was particularly useful because we changed from ISO 31000:2009 to ISO 31000:2017 as source standard, and some modifications and adjustments had been made.

Step 4: Identify and factorize outcomes from the common purposes and attach them to the related goals

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. The outcomes of each process had to be factorized or merged, according to convenience and expert judgement, in order to define from 3 to 7 outcomes per process, and thus to follow the recommendations of ISO/IEC TR 24774 [33].

In some cases, the common purposes identified during step 3 were considered as the process outcomes and were attached to the related domain goals. In other cases, where a more detailed granularity level is wished, the common purpose supported the definition of process purpose. Grouping of elementary statements then enable to identify outcomes.

Step 5: Group activities together under a practice and attach it

TOP MANAGEMENT Process		
TOP.01 Leadership		
COMMON Processes		RISK MANAGEMENT Processes
COM.01 Communication management	COM.07 Non-conformity management	RIS.01 Risk criteria definition
COM.02 Documentation management	COM.08 Operational planning	RIS.02 Risk identification
COM.03 Resource management	COM.09 Operational implementation and control	RIS.03 Risk analysis
COM.04 Improvement	COM.10 Performance evaluation	RIS.04 Risk evaluation
COM.05 Internal audit	COM.11 Monitoring	RIS.05 Risk treatment
COM.06 Review		RIS.06 Reporting and recording

Fig. 2. IRMIS PRM proposed list of processes.

to the related outcomes

The original input of the Transformation process (the statements from ISO 31000) sometimes contains information describing activities that should be conducted for implementing the processes. According to the number and level of detail of these activities, they were grouped as practices. When there were no detailed information within the statements of ISO 31000, practices were deduced from the outcomes. Each practice represents a functional activity of the process. When implemented, a practice contributes to the achievement of at least one outcome of the performed process. During this step, we linked these activities or practices to the related outcomes and we maintained traceability between each practice and the initial set of elementary statements. Indeed, it is possible that several elementary statements are related to only one practice of a process. The goal trees enable to keep that in mind for further activities, in particular, when questionnaires are being developed for supporting process assessment.

Step 6: Allocate each practice to a specific capability level

For each process, we review the practices and their linked outcomes in order to confirm that they contribute to the process performance attribute (capability level 1) of their associated process, and not to capability levels upper than 1. We ensured that our process descriptions are such that no aspects of the measurement framework beyond level 1 are contained or implied and thus, that the created process reference and process assessment models comply with ISO/IEC 33004 Requirements for process reference, process assessment and maturity models.

Step 7: Phrase outcomes and process purpose

In order to create a process reference model that follows the guidelines of ISO/IEC TR 24774, each outcome has to be phrased as a declarative sentence using verbs at the present tense. Then, the purpose is phrased or refined if phrased when the process is identified to state a high-level objective for performing the process and provide measurable and tangible benefits to the stakeholders through the expected outcomes (process assessment concern). From the risk management sub-processes of ISO FDIS 31000 (Risk identification, Risk analysis, etc.), process purposes are proposed and provide a sound basis for the phrasing (kept as it is when appropriate and compliant with ISO/IEC 33004 requirements). We also checked that the set of outcomes is necessary and sufficient to achieve the purpose of the process.

The resulting IRMIS PRM is suitable for use in process assessment performed in accordance with the requirements for a PRM described in Clause 6.2 of ISO/IEC 33004.

- The declaration of the domain is: Integrated Risk Management for IT Organizations.
- The description of the processes is provided in the IRMIS PRM.
- The IRMIS PRM describe at an abstract level the processes implied by ISO 31000. The purpose of the IRMIS PRM is to facilitate the development of a process assessment model for integrated risk

management in IT Organizations.

- A description of the relationship between the processes defined within the IRMIS PRM is supported by a figure collecting all the processes by process groups.

The process descriptions are unique. The identification is provided by unique names and by the identifier of each process of the IRMIS PRM. Processes are described in terms of its purpose and outcomes. For all processes, the set of process outcomes are necessary and sufficient to achieve the purpose of the process. No aspects of the ISO/IEC 33030 Measurement Framework beyond level 1 are contained in process descriptions.

Once the PRM determined, critical aspects of integration with other selected ISO standards were considered. The selected relevant standards were ISO 21500 and ISO/IEC 27001 supported by ISO/IEC 27005. ISO 21500 has dedicated processes for Risk identification, Risk assessment, Risk treatment and Risk control. ISO/IEC 27001 does not provide much detail, but ISO/IEC 27005 does, with Risk identification, Risk analysis, Risk evaluation, and Risk treatment. So we used these standards for a PAM providing multi-application views. We selected the Capability Measurement Framework provided by the standard as we consider Capability as the quality characteristic considered in our work.

Step 8: Phrase the Base Practices attached to Outcomes

Once the purpose and outcomes of a process is phrased, the process reference model is considered stable enough to phrase the base practices. Base practices are phrased as actions, starting with a verb at the infinitive, according to ISO/IEC 24774. During steps 8 and 9, we pay particular attention to choose wording that suits and that is commonly used for dealing with risk management in organizations in order to ensure a successful adoption of the models. The context for Risk management will target project management in ISO 21500 and information security in ISO/IEC 27001.

Step 9: Determine Work Products among the inputs and outputs of the practices

A work product is an artefact associated with the execution of a process. During the steps 1 and 5, work products can be identified. For instance, it is very clear that the main output work product for Risk identification is a “comprehensive list of risks”. It is mentioned as “Risk register” in ISO 21500. For Risk analysis process, the main output is the list of “Analysed risks with the determined level of risks”: it is mentioned as “Measured risks” in ISO 21500, and as “List of risks with value levels assigned” in ISO/IEC 27005.

The following paragraphs present an extract of the PRM, followed for each process by a table providing the PAM (respective Tables 6–8); each table present a process with multiple views presenting the mapping with the other standards considered with ISO 31000; it is illustrated for ISO 21500 and ISO/IEC 27001 for Risk assessment in ISO 31000, meaning 3 processes: Risk identification, Risk analysis and Risk evaluation. The idea to provide views is to extend the ISO 31000 to the

Table 6
The Risk identification 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)	BP1. Gather relevant and up-to-date information for the identification of risks (appropriate background information where possible)	Information comes as the project progresses through its life cycle	Information comes from the information security risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system
BP2 (Out 1)	BP2. Select context relevant risk identification tools and techniques.		
BP3 (Out 2)	BP3. Examine a set of factors for identifying risks; (Tangible and intangible sources of risk, Causes and events, Threats and opportunities, vulnerabilities and capabilities ,...)		
BP4 (Out 3)	BP4. Identify risks based on factors of risks.	Identification of risks with a potential negative impact (threats) Identification of risks with a potential positive impact (opportunities)	Identification of assets Identification of threats Identification of existing controls Identification of existing vulnerabilities Identification of consequences
Input Work Products	Risk management plan	Project plans	Scope and boundaries for the risk assessment, list of constituents with owners, location, function, etc.
Output Work Products	Risk register (list of risks)	Risk register	A list of incident scenarios with their consequences related to assets and business processes identification

context of the other selected ISO standards, but to keep the ISO 31000 structure as the core standard. The management systems mechanisms help the integration, but the specifics need to remain as such. The assessor will then be able to collect data with the appropriate context.

Inputs and output work products are indicative. The measurement framework of our PAM is based on the ISO/IEC 33020 one proposing a process measurement framework for assessment of process capability.

The Risk identification process description

Process ID RIS.02
ID
Name Risk identification
Purpose

Outcomes The purpose of the Risk identification process is to find and describe risks that might help or prevent an organization from achieving its objectives.
As a result of successful implementation of this process:
1. Relevant information and risk identification techniques are selected.
2. Factors of risks and their relationships are examined.
3. Risks are identified, based on factors of risks.

Table 7
The Risk analysis process description and views in the IRMIS PAM.

	ISO 31000 view	ISO 21500 view	ISO/IEC 27001 view
Process ID	RIS.03		
Process Name	Risk analysis		
BP1 (Out 1)	BP1. Select analysis techniques that are appropriate depending on circumstances and intended use.		Risk analysis methodologies (qualitative, quantitative)
BP2 (Out 2)	BP2. Identify the factors of risks to consider. Note: These factors can be: likelihood of events and consequences, the nature and magnitude of consequences, complexity and connectivity, time-related factors and volatility, pace of change, effectiveness of existing controls, sensitivity and confidence levels, influences (any divergence of opinions, biases, perceptions of risk and judgements; additional influences: the quality of the information used, the assumptions and exclusions made, any limitations of the techniques and how they are executed).		
BP3 (Out 3)	BP3. Determine a level of risks considering uncertainties, risk sources, consequences, likely-hood, events, scenarios, controls and their effectiveness	Estimate the probability of occurrence of each risk Estimate the corresponding consequence for project objectives	Assess consequences of risks (assets identification, assessment of business impact in terms of Confidentiality, Integrity, Availability) Assess incident likelihood (likelihood of incident scenarios : quantitative or qualitative) Determine the level of risks Issue a list of risks with value levels assigned
BP4 (Out 4)	BP4. Record risk analysis results.		
BP5 (Out 5)	BP5. Communicate risk analysed results to decision makers.		
Input Work Products	Risk register (list of risks)	Risk register	List of identified relevant incident scenarios
Input Work Products		Project plans	
Output Work Products	Analysed risks (level of risks)	Measured risks	List of risks with value levels assigned

Table 8
The Risk evaluation process description in the IRMIS PAM.

	ISO 31000 view	ISO 21500 view	ISO/IEC 27001 view
Process ID	RIS.04		
Process Name	Risk Evaluation		
BP1 (Out 1)	BP1. Compare analysed risks to risk criteria.		
BP2 (Out 2)	BP2. Decide what to do for each risk	Risks are prioritized considering factors such as timeframe and key stakeholders' risk tolerance	Decisions are mainly based on the acceptable level of risk
BP3 (Out 3)	BP3. Record the evaluated risks issued from the comparison of analysed risks to risk criteria.		
BP4 (Out 4)	BP4. Communicate the evaluated risks to stakeholders		
BP5 (Out 5)	BP5. Validate the evaluated risks at appropriate levels of the organisation		
Input Work Products	Analysed risks	Measured risks (probability and consequences)	List of risks with value levels assigned
Input Work Products	Risk criteria		Risk evaluation criteria
Output Work Products	Evaluated risks record	Prioritized risks	List of prioritized risks

Comments on the Risk identification process: This process is part of the overall Risk assessment to be performed by any organization dealing with Risk management. Risk assessment encompasses Risk identification, Risk analysis and Risk evaluation and as stated in ISO 31000: *“it should be conducted systematically, iteratively and collaboratively”*. Risk identification is key, with a relevant and up-to-date information to be used for identifying risks. For integration purposes, several types of risks are identified, considering the type of activity which is performed: business risks, project risks, information security risks, etc.

The Risk analysis process description

Process ID RIS.03

Name Risk analysis

Purpose The purpose of risk analysis is to determine a level of risk from analysis techniques and factors of risks.

Outcomes As a result of successful implementation of this process:

1. Appropriate analysis techniques are selected.
2. Factors of risks are considered including influences.
3. A level of risk is determined.
4. Risk analysis results are recorded.
5. Risk analysis results are communicated to decision makers.

Comments on the Risk analysis process: This process is focusing on the comprehension of risks, in order to determine a level of risk, prepare the decision-making of the Risk evaluation process. It is based on the identified risks, and produces a list of analysed risks with a level of risks.

The Risk evaluation process description

Process ID RIS.04

Name Risk evaluation

Purpose The purpose of risk evaluation is to support decisions.

Outcomes As a result of successful implementation of this process:

1. The significance of risks is determined by comparing analysed risks to risk criteria.
2. A decision is made based on the determined significance of risks
3. Evaluated risks are recorded
4. Evaluated risks are communicated at appropriate levels of the organisation
5. Evaluated risks are validated at appropriate levels of the organisation

Comments on the Risk evaluation process: This process is dealing with prioritization of risks, in order to decide what to do for each risk: do nothing further, consider risk treatment options, investigate more on some risks, etc.

In order to check the fulfilment of ISO/IEC 330xx requirements in designing the IRMIS PAM, a first validation loop of experts have been performed in order to validate the content and assure its quality with a systematic review of the following criteria:

- An outcome is targeting capability level 1 only;
- An outcome can be identified as an artefact, a change of state or a meeting of constraints;
- The wording is clear and appropriate for all PAM components;
- The vocabulary used in the PAM is consistent;
- Each process is defined with the following characteristics mind-set: assessability, interoperability, integration, completeness, adoption and applicability.

This approach has enabled some improvements and refinements in the wording and in the consistency of the used vocabulary in particular. The same approach is used for all processes of the PAM.

5. Conclusion

This paper has presented the work performed in order to develop an ISO/IEC 33004 compliant Integrated risk management in IT Organizations (IRMIS) PRM and PAM, based on ISO 31000 (international reference on Risk management) by applying a Transformation process. The resulting IRMIS PRM & PAM is covering the risk management guidance recommended by the last Final draft of the ISO 31000 International Standard for the high level objectives of the PRM, and detailed and context-based indicators within the PAM, for process assessment purposes. The next stage of our research will follow remaining steps of the DSRM in order to evaluate the results, and communicate them. This will allow companies to assess the capability of their risk management processes from an ISO-many fold perspective and then, to use the results as a basis for process improvement. A first loop of validation has been performed with process assessment, management systems in IT Organizations and project management experts. This validation loop was particularly relevant after having updated all content of our works because of the selection of the ISO 31000 latest revision. More validation loops will be performed with risk management experts (in particular for Information Security) opinion by collecting feedback. Other R&D experts working in process models for other domains are planned to be consulted. Demonstration and evaluation will also be carried out in industry. Different Risk management officers in IT Organizations (including Security officers of Information Systems, IT Project Managers and IT Service Managers) will be

consulted about the suitability of the structure and contents of the IRMIS PRM and PAM. They will be asked to use these models in order to evaluate their effectiveness. Statement and goal trees could be used as a tool supporting validation of the models. All changes requested and comments obtained from the validation process will be incorporated into the final version of the IRMIS Process Models.

Acknowledgements

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

References

- [1] ISO/IEC 15504: Information technology, Process assessment, Parts 1-10, – International Organization for Standardization, Geneva, 2003 2012.
- [2] ISO/IEC 330xx: Information Technology, Process Assessment, International Organization for Standardization, Geneva, 2013 2017.
- [3] ISO/IEC 15504-5: Information Technology, Process assessment, An Exemplar Software Life Cycle Process Assessment Model, International Organization for Standardization, Geneva, 2012.
- [4] ISO/IEC 15504-6: Information Technology, Process assessment, An Exemplar System Life Cycle Process Assessment Model, International Organization for Standardization, Geneva, 2013.
- [5] ISO/IEC 15504-8: Information Technology, Process assessment, An Exemplar Process Assessment Model For IT Service Management, International Organization for Standardization, Geneva, 2012.
- [6] ISO/IEC 33071: TS Information Technology, Process Assessment, An Integrated Process Capability Assessment Model For Enterprise processes, International Organization for Standardization, Geneva, 2016.
- [7] ISO/IEC 33072: TS Information Technology, Process Assessment, Process Capability Assessment Model For Information Security Management, International Organization for Standardization, Geneva, 2016.
- [8] ISO/IEC 33073: TS Information Technology, Process Assessment, Process Capability Assessment Model For Quality Management, International Organization for Standardization, Geneva, 2017.
- [9] ISO/IEC 30105-2: TS Information Technology, IT Enabled Services-Business Process Outsourcing (ITES-BPO) lifecycle processes, Process Assessment Model (PAM), International Organization for Standardization, Geneva, 2016.
- [10] Automotive Spice, 2016. (online: accessed 22-January-2018) <https://goo.gl/BNu8c2>.
- [11] Isaca: COBIT Process Assessment Model (PAM): Using COBIT 5 (ISBN:1604202718 9781604202717) (2013).
- [12] TIPA for ITIL, 2015. (online: accessed 22-January-2018) <https://goo.gl/EA9NMh>.
- [13] M. Lepmets, F. McCaffery, P. Clarke, Development and benefits of MDevSPICE[®], the medical device software process assessment framework, *J. Softw* 28 (9) (2016) 800–816.
- [14] ISO/IEC 27001: Information technology, Security techniques, Information Security Management Systems – Requirements, International Organization for Standardization, Geneva, 2013.
- [15] ISO/IEC DIS 20000-1: Information Technology, Service management, Part 1: Service management System Requirements, International Organization for Standardization, Geneva, 2011.
- [16] ISO 9001: Quality management systems, Requirements, International Organization for Standardization, Geneva, 2015.
- [17] ISO/IEC ISO 21500: Guidance on project management, International Organization for Standardization, Geneva, 2012.
- [18] B. Barafort, A.L. Mesquida, A. Mas, Integrating risk management in IT settings from ISO standards and management systems perspectives, *Comput. Standards Interfaces*. 54 (2016) 176–185.
- [19] B. Barafort, A.L. Mesquida, A. Mas, How to elicit Processes for an ISO-based Integrated Risk Management Process Reference Model in IT Settings, *European Conference on Software Process Improvement*, Springer, Cham., 2017, pp. 43–57.
- [20] B. Barafort, A.L. Mesquida, A. Mas, Developing an Integrated Risk Management Process Model for IT Settings in an ISO Multi-standards Context, *International Conference on Software Process Improvement and Capability Determination*, Cham, Springer, 2017, pp. 322–336.
- [21] ISO 31000: Risk management – Principles and guidelines (2009).
- [22] ISO FDIS 31000: Risk management – Principles and guidelines (2017).
- [23] B. Barafort, A. Renault, M. Picard, S. Cortina, 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.
- [24] K. Peffers, T. Tuunanen, M. Rothenberger, S. Chatterjee, A design science research methodology for information systems research, *J. Manage. Inf. Syst.* 24 (3) (2008).
- [25] L. Buglione, A. Abran, C.G. von Wangenheim, F. McCaffery, J.C.R. Hauck, Risk Management: Achieving Higher Maturity & Capability Levels through the LEGO Approach, *Software Measurement and the International Conference on Software Process and Product Measurement (IWSM-MENSURA)*, 2016 Joint Conference of the International Workshop on, IEEE, 2016, pp. 131–138.
- [26] ISO, Economic benefits of standards – International case studies (ISBN 978-92-10556-7) (2014).
- [27] ISO Survey, (online: accessed 22-January-2018), <https://www.iso.org/the-iso-survey.html>, (2016) (online: accessed 22-January-2018).
- [28] S.T. MacMahon, F. McCaffery, F. Keenan, The MedITNet assessment framework: development and validation of a framework for improving risk management of medical IT networks, *J. Softw.* 28 (9) (2016) 817–834.
- [29] D. Proença, J. Esteves, R. Vieira, J. Borbinha, Risk Management: A Maturity Model Based on ISO 31000, *Business Informatics (CBI)*, 2017 IEEE 19th Conference on, Vol. 1 IEEE, 2017, pp. 99–108.
- [30] ISO/IEC 27005: Information technology, Security techniques, Information Security Risk Management – Requirements, International Organization for Standardization, Geneva, 2011.
- [31] P.J. Denning, A New Social Contract for Research, *Commun. ACM* 40 (2) (1997) 132–134.
- [32] S. March, G. Smith, Design and natural science research on information technology, *Decision Supp. Syst.* 15 (4) (1995) 251–266.
- [33] ISO/IEC TR 24774: Software and systems engineering, Life cycle management, Guidelines For Process Description, International Organization for Standardization, Geneva, 2010.



Béatrix Barafort graduated as a Software Engineer in the Conservatoire National des Arts et Métiers (France) and has worked from 1988 to 1996 in a software house in Lyon for software development projects in banks and insurance companies. Then she joined Public Research Centre Henri Tudor in Luxembourg where she has led R&D process assessment and improvement projects based on the ISO/IEC 15504 standard (Process Assessment), mostly in Software Engineering and IT Service Management. At the beginning of 2015, the Tudor centre merged with another public research centre to become the Luxembourg Institute of Science and Technology (LIST). Béatrix is now heading an R&D Group on “Service and Process Governance” encompassing the TIPA[®] initiative (open framework for process assessment including TIPA for ITIL). She is actively involved in standardization activities in ISO/IEC JTC1 SC7 (Software and Systems Engineering with Process Assessment as a particular interest) and in ISO/IEC JTC1 SC40 (IT Service Management and IT Governance). She was editor of the published ISO/IEC 20000-4:2010 standard for an IT Service Management Process Reference Model.



Antoni-Lluís Mesquida is an assistant lecturer with a doctoral degree of project Management and Software Quality at the University of the Balearic Islands. His research interests include Software Process Improvement, Project Management and IT Service Management. He is a member of the MiProSoft research group. He has participated in the QuaSAR project, a soft-ware process improvement program in small software companies in the Balearic Islands. He received his PhD in Computer Science from the University of the Balearic Islands.



Antonia Mas is University Lecturer at the University of the Balearic Islands. Her teaching activity is centered in the field of Software Engineering, Software Quality and Project Management. She is currently the director of Master in Computer Science and three postgraduate courses related to Project Management. She is a member of the MiProSoft research group. Her re-search interests cover the fields of Software Process Improvement, Project Management and IT Service Management. The results of her research group have been applied in successive editions of the QuaSAR Project, a project for the improvement of software development processes in small software companies in the Balearic Islands. She is an ISO/IEC 15,504 assessor and is focused on assessing small companies. She received a degree in Computer Science by the Autonomous University of Barcelona (UAB) and a PhD in Computer Science by the University of the Balearic Islands (UIB).

4.3 Research contribution C3


- C3. Barafort, B.; Mesquida, A.L. & Mas, A. **ISO 31000-based Integrated Risk Management Process Assessment Model for IT Organizations**. *Journal of Software: Evolution and Process* .To be published, 2018.

4.3.1 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.

4.3.2 C3 Paper

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

Béatrix Barafort¹ | Antoni-Lluís Mesquida²  | Antònia Mas²

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

²Department 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 domains¹⁻⁴; these various initiatives are based on the ISO Process assessment standard series concepts⁵; they rely on a very structured and systematic approach for process assessment and guided process improvement.

Our research works⁶ 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 21500¹⁰ (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 al⁶). 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 31000¹¹ 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 Process¹³ for designing PRMs and PAMs fulfilling the Process Assessment ISO standard requirements for developing PRMs and PAMs.¹⁴ The ISO/IEC 27005¹⁵ 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 al¹⁸ 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 al¹⁹ 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. Roy²¹ 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 SEI²² 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 studies²³ 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 al²³ 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 PMBoK²⁷ 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 al²⁸ 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 Manifesto²⁹ "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 16085³⁰: "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&MM³² 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 has its own ISO standard⁵ 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 Framework³⁶ 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 survey³⁸ 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 al³⁹ 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 27013⁴⁰ 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 33072⁴¹), for ITSM (ISO/IEC 15504-8³) and for quality management based on ISO 9001 (ISO/IEC 33073⁴²). 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 73⁴⁵).

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 20000-10⁴⁶ and ISO/IEC 27000⁴⁷ 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 33004¹⁴ 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 Decomposed Elementary 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 standard⁴² which is the latest version of a PAM published by ISO; only two processes are derived from ISO/IEC 33072⁴¹ for



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	COM.01 Communication management	Communication management
6.2 Communication and consultation		
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	9.2 Risk modification
6.5.3 Preparing and implementing risk treatment plans	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

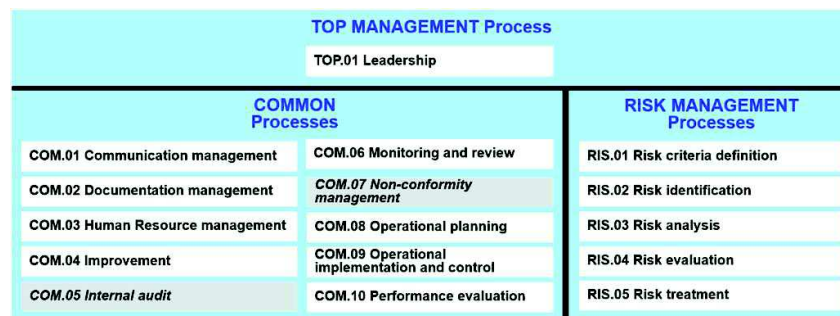


FIGURE 2 IRMIS PRM proposed list of processes

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, ISO/IEC 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 (WISM-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.* 2018;e1984. <https://doi.org/10.1002/smr.1984>

5. Discussion and conclusion

This chapter presents the discussion related to the research challenges addressed by this PhD thesis, followed by the conclusion and future works.

5.1 Discussion

Several challenges have been addressed in the performed research of this PhD thesis and are discussed in this paragraph. These challenges are related to the main research question *“how to improve risk management processes in IT settings from an integrated and management system perspective in multiple ISO standards”*. Throughout this PhD thesis, the following research objectives (ROx) related to their respective research question (RQy) were addressed:

- RO1: investigation and comparison of risk management activities throughout selected ISO standards targeting management systems,
- RO2: showing that a centralized and management systems approach based on processes contributes to integration in a process-centric risk management mindset,
- RO3: proposal of means to improve risk management processes in IT settings,

and artefacts were designed. The next paragraphs discuss the outcomes of the PhD with the various artefacts that were produced and presented throughout the publications presented in chapter 0, according to the reminded main objectives.

5.1.1 Investigation and comparison of risk management activities throughout selected ISO standards targeting management systems

Risk management activities are present in many ISO standards. As the notion of risk is generic and can target any business, any sector, any area of companies, and competitiveness is critical, it is important to identify these activities. In this PhD's work, risk management activities have been investigated in various ISO standards: in ISO 31000 as the main line, and in a set of standards which are relevant for IT settings in a management system's mindset: Annex SL, ISO 9001, ISO 21500, ISO/IEC 20000-1 and ISO/IEC 27001, with ISO/IEC 27005 as a complement.

The main achievement related to the objective of investigation and comparison of risk management activities has been their identification and a comparison of clauses against ISO 31000 ones. The detailed mapping is in section 4 of [C1]. It is followed by a description of relations or connection points among risk-based activities. It has shown that all standards tackle the notion of context, as well as the importance of Leadership, and follow the PDCA loop, with other common points such as communication and consultation, resources, monitoring and review. ISO 31000 emphasises dedicated risk management activities with an overall risk management process tackling risk identification, risk assessment with risk identification, risk analysis and risk evaluation, and finally risk treatment. Annex SL, ISO 9001 and ISO/IEC 20000-1 are not targeting in detail these risk management activities but from an overall perspective, whereas ISO 21500 and ISO/IEC 27001 are more aligned with the detailed statements of ISO 31000.

The investigation and comparison of risk management activities against ISO 31000 clauses confirmed the position of ISO 31000 as the main line of this PhD's work. It also confirmed that ISO 31000, even if it is not a management system standard in the way of a certification (there are no "SHALL" statements), has a similar structure as the one of a management system and facilitates the integration with management systems such as ISO 9001, ISO/IEC 20000-1 and ISO/IEC 27001 (which have to follow the HLS imposed by ISO to MSSs). To act from a preventing perspective is seen via a risk-based thinking in all MSSs. Top management has to decide how to introduce this in the organization, with the appropriate granularity and formalism level according to its context. While each type of risk has to be addressed on a dedicated way, the same mechanisms can be applied from the guidance of ISO 31000. The process approach principle is also present in all targeted standards: this is a major argument for integration and organizational facilitator, as well as the PDCA methodology. As stated in ISO 9001, a *"process approach enables an organization to plan its processes and their interactions"*, and the *"PDCA cycle enables an organization to ensure that its processes are adequately resourced and managed, and that opportunities for improvement are determined and acted on"*. With risk-based thinking, it *"enables an organization to determine the factors that could cause its processes and its quality management system to deviate from the planned results, to put in place preventive controls to minimize negative effects and to make maximum use of opportunities as they arise"*. Even if ISO 21500 is not a MSS, it remains relevant as project management is a key domain in IT settings, with embedded risk management related to processes similar to ISO 31000 activities.

Globally speaking, the ISO 31000 principles are reflected in the Annex SL, ISO 9001, ISO 21500, ISO/IEC 20000-1 and ISO/IEC 27001. The mapping that has been performed could have been executed with a supporting tool to facilitate the comparison and automate it once the coding of the content with clauses done. That would limit the risk of errors. This could also be of particular help when there are new versions of revised standards to include. Nevertheless, the main principles remain the same and secure the analysis.

5.1.2 Showing that a centralized and management systems approach based on processes contributes to integration in a process-centric risk management mindset

The main achievements related to the objective of showing that a centralized and management systems approach based on processes contributes to integration in a process-centric risk management context are related to:

- the terminology for integrated risk management in a multi-ISO standards context (see chapter 6: Annex – Terminology tables),
- the identification of elementary statements from ISO 31000 (see chapter 0) in order to group them in requirements trees (see chapter 0), enabling to identify processes. These processes have two main purposes: on the one hand to cover mechanisms for managing systems, and on the other hand to deal with specific risk management activities.

In this PhD's work, the integration aspect is paramount. This is the reason why the integration based on terminology and structuring is essential. The author has studied main definitions of risk management, with a comparison to similar terms in the studied standards. As ISO standards are developed on the basis of international consensus, the terminology equipping these standards is proven and recognized. The author selected most definitions from ISO 31000 and ISO Guide 73. Terminology tables (see chapter 6) specify the selected definitions.

ISO has performed a dedicated effort for harmonizing MSSs by imposing a common structure for all of them, with compulsory clauses and requirements. Moreover, the process-based approach drives integration by its transversal nature, with outputs from a process being inputs for other ones and so on. Even if the 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. The various mappings performed by the author confirmed this as well as two intermediary artefacts that help identifying integration aspects and candidate processes for transcribing ISO 31000 as a full process-based model: these artefacts are a list of elementary statements derived from the sentences of each clause (see chapter 0), and a set of Requirements trees grouping elementary statements by similar topics (as required by the Transformation process described in [6] and explained in the followed research method in chapter 0 with the Design and development activity). These similar topics were guided by Annex SL for MSSs on the one hand, and on specific risk management activities on the other hand (see requirement trees examples for specific risk management processes in chapter 0), and they helped eliciting processes. ISO 31000 being a guideline standard and not a requirements one, some identified processes labelled as "common processes" are not existing in ISO 31000 (no statements related to *Audit* neither *Non-conformity management*). The author chose to let them appear in the process map (see the process map in 3.3, [C2] and [C3], as well as in the PAM in Chapter 0) from an integration perspective with MSSs such as ISO 9001, ISO/IEC 27001 and ISO/IEC 20000-1. The process name has also to be clearly identified and understood by practitioners. The author has also made choices based on the current terminology of ISO 31000. For instance, the Review concept is not associated with the term Management in our proposed PRM, 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; in this case, the author kept the label Performance evaluation in the proposed process model as it is more explicit.

The review of literature has shown that the idea of using management systems mechanisms for integration purposes had never been realized for a risk management framework based on ISO 31000 fulfilling ISO requirements for process reference and process assessment models. Taking profit from ISO standards has several facets such as terminology, structuring with integration factors coming from management systems mechanisms and reusing common pieces when relevant. The author claims that this approach of integrated management system is for IT settings; it is the problem to be solved and the

motivation of this PhD thesis work. Market demands from IT settings (as a reminder, IT settings meaning any IT department or IT company needing to integrate risk management activities) were targeting ISO 9001, ISO/IEC 20000-1 and ISO/IEC 27001; they are very popular management systems, documented as integration vectors in literature as mentioned in [C1]. Like ISO 21500 for project management, some of these standards are IT-related and some of them are non-IT related ones. But they have been selected by the author because they are significant for many companies and as previously mentioned, they were reported back by practitioners. It is true that the IT aspects are not predominant in the results of this PhD thesis but in the same way as ISO 31000, ISO 9001 and ISO 21500 are not IT or software specific, ISO 9001 in particular is very demanded in IT settings; and like ISO 21500, it is transversal.

5.1.3 Proposal of means to improve risk management processes in IT settings

The main achievements related to the objective of proposing means to improve risk management processes in IT settings are dealing with intermediary artefacts such as:

- The Transformation process applied to ISO 31000 and selected ISO standards (see in 3.3 and [C2])
- The goal trees for identified processes (see in Chapter 0 and in [C3])

and the main artefacts such as:

- The PRM for Integrated Risk Management for IT Settings (IRMIS)
- The PAM for IRMIS (see in Chapter 0, and some process descriptions in [C2] and [C3]).

These main artefacts have been created in an assessment and improvement context, as the TIPA Framework. They can be used for assessment purposes, with the TIPA method enabling to identify strengths, weaknesses, opportunities and threats (SWOT analysis) and to formulate recommendations for improvement.

Based on the elicited processes mentioned in previous section (5.1.2), the PRM has been populated with purpose and outcomes for each process. The Transformation process has been applied for all processes, with detailed indicators described for each process, meaning base practices contributing to the outcomes, as well as inputs and outputs work products (so they constitute the PAM for the process dimension, as requested by ISO/IEC 33004; the measurement framework dimension for the IRMIS PAM is provided by the capability measurement framework proposed in ISO/IEC 33020 [109]). For leadership and common processes, existing processes from ISO/IEC 33072 and ISO/IEC 33073 were reused; the Transformation process has been adapted because some mappings have been performed between Requirement trees and existing process descriptions: the results were included in the Goal trees where the outcomes are described. Then the existing outcomes were logically reused from ISO/IEC 33072 and ISO/IEC 33073. For specific risk management processes, the Transformation process has been applied as such, as described in [C2]. It is important to note that the author has chosen to name the system: “Risk management framework” in each place where “xxx management system” was used in the common processes described in existing PRM and PAM (respectively “Process capability assessment model for

information security management” for ISO/IEC 33072 and “Process capability assessment model for quality management” for ISO/IEC 33073), as ISO 31000 is not management system enabling an ISO certification like for i.e. ISO 9001.

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 author decided to propose a dedicated process and to adopt the same documentation management mechanisms as the ones of this process in MSSs PRMs and PAMs (as in ISO/IEC 33072 and ISO/IEC 33073).

The IT organizations specificities are not visible in the elicitation of processes at the PRM level. A particular attention was paid on these aspects at the PAM level 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, ISO/IEC 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.

The review of literature has shown that the idea of proposing a PRM and a PAM enabling process assessment in an improvement perspective has never been realized for integrated risk management based on ISO 31000. The IRMIS PRM and PAM fill a gap in terms of risk management with integration aspects conveyed by terminology, process-approach, and management system mechanisms. A particular attention has been paid with some aspects for favoring adoption and assessability (terminology adapted to risk management and management system, limited number of processes...). By its nature fulfilling ISO/IEC 33004 requirements, the IRMIS PRM fosters interoperability, efficiency and effectiveness; some communities (ISO and industry) have already advocated the usefulness and relevance of process models for process assessment in process management, improvement and performance contexts. In July 2018, ISO has launched an invitation to ISO experts for two workshops aiming at developing an International Workshop Agreement on “*Using ISO 31000 guidance on risk management in management systems*” [111]. This initiative is largely aligned with these PhD thesis outcomes; the author is considering joining for introducing them to this ISO-related risk management community, in relation with management systems.

For the PRM and PAM design, the mappings, requirements trees and goal trees have been performed with office suite tools. It would have been more efficient to use a supporting software tool to facilitate the way from one step to the other (for instance from elementary statements to requirements tree, and from requirements tree to goal tree) and to avoid mistakes. The automation would facilitate the work once the coding is performed because the Transformation process steps are important as they favour a certain level of quality of the process models.

5.2 Conclusion and future works

5.2.1 Conclusion

In current IT organizations, GRC activities play an important part with risk management as a key challenge in several areas in which the nature of risk differs (they can be related to quality, projects, IT services, Information security). Risk management has to be organized, to be part of and integrated within the management system(s) of the company. In order to address all these challenges, this PhD thesis proposes an integrated risk management approach in IT settings with ISO standards, with two main artefacts: a Process Reference Model and a Process Assessment Model, based on: the international standard on Process assessment for designing process models (ISO/IEC 33004 [77]), on the international reference standard in risk management: ISO 31000, and in relation with ISO standards demanded by IT organizations in the industry: ISO 9001 for quality management, ISO 21500 for project management, ISO/IEC 20000-1 for IT service management and ISO/IEC 27001 for information security management. Both artefacts contribute to an Integrated Risk management Improvement Framework in ISO settings with ISO standards and are the main research contribution of this thesis.

This research contributes to the literature of various domains as it associates them in several ways; the various contributions relate mainly to the following literature: risk management and integrated risk management, management systems, capability and maturity models, process assessment and process improvement. The research also contributes to the literature on ISO standards, with a particular focus on management systems and process-based approach standards, including such main relevant IT related management system standards in: service management and information security management.

The research methodology used in this work involves a DSR approach with the problem stated from which the design of the main artefacts (IRMIS PRM and PAM) was triggered; additional intermediary artefacts (mappings, terminology tables, elementary statements, requirements trees, goal trees) were designed for supporting the overall approach: in particular a Transformation process has been followed to derive the process purpose, outcomes and base practices from the elementary statements of the Ariane's thread of the research works: the ISO 31000 standard. A first complete iteration according to DSR approach was performed; more iterations are to be performed to improve the main artefacts (IRMIS PRM and PAM). Academic researchers and industry practitioners feedbacks are considered throughout scientific and professionals communications, as well as with standardization works in the ISO community.

5.2.2 Future works

Future research avenues can progress along different lines. In particular:

- The consolidation of the results with more DSR iterations is foreseen. This will enable to refine the PRM and PAM. These iterations will also enable to present the research outcomes to the ISO community in two experts groups and get more feedbacks:
 - on the one hand in the ISO/IEC JTC1 SC7 WG10 on process assessment in order to propose a new PRM and PAM in the ISO/IEC 330xx series (Two options can be proposed: whether

the PRM and PAM covers only the ISO 31000 standard, or the complete IRMIS PRM and PAM which proposes additional views with ISO 21500 and ISO/IEC 27001.).

- on the other hand in the new International Workshop Agreement on “Using ISO 31000 guidance on risk management in management systems” [111], the research contribution of the PhD thesis work on integration of risk management with management systems common processes can bring some guidance on risk management aligned with ISO 31000.
- These ISO perspectives can be additional benefits of ISO standards for industry related to risk management, and also to quality management, project management, service management and information security management in a management system context.
- Revisions of the selected standards for this PhD thesis can also be the opportunity for new DSR iterations and improvements of the IRMIS PRM and PAM.
- Integration is a key challenge in this PhD thesis and has been tackled from the management systems perspective with a systematic methodology (Transformation process), for considering statements from the ISO 31000 standard on risk management with a GORE technique. This enabled to align statements with the process elements of existing PAMs [52, 85] for common processes related to management systems, and also to derive purpose, outcomes and base practices for specific risk management processes, on a more detailed way than existing PAMs proposing only one dedicated process for risk management. With the growing complexity and market demands for standards such as ISO ones targeting management systems certification, and regulations imposed by legislators, their combined translation into integrated C&MM(s) become more difficult. New research challenges appear with the integration of several domains where risk management is just one case. Then not only requirements engineering play an important part, but also other disciplines such as regulatory compliance; the demonstration of traceability is then an additional key challenge to tackle, beyond integration when there are multiple standards and regulations to address.
- Integration could also be tackled from a harmonization point of view, with an ontology to represent the knowledge. An ontology could clarify the risk management domain’s structure of knowledge, and enable knowledge sharing; several ontologies could be developed to complete the generic risk management one in order to cover multiple domains such as quality management, project management, service management and information security management. Common topics for management systems could then be represented only once. These ontologies could be the basis for formalizing processes of the IRMIS PRM and PAM and help updating them.
- Situational factors related to risk management 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. Key situational elements affecting risk management in IT settings could be investigated and a reference framework with classifications and factors that inform the risk management processes could be proposed.
- Process assessments based on the IRMIS PAM in various sectors could be compared in order to investigate further its relevance and to determine potential adaptations in IT settings for each specific sector as the nature of risk varies.

- Finally, these PhD thesis works contribute to the enhancement of the TIPA Framework and can extend it on several ways:
 - Populate the TIPA library of process models with an additional PRM and PAM (IRMIS) that can be aligned with other MSSs-based PRM and PAM, and expanded with more IT settings related ISO standards.
 - Contribute to the Transformation process on-going enhancement with an additional case of multiple sources to deal with and the use of mappings between the statements of ISO 31000 and existing PAMs description of common processes for management systems such as in ISO/IEC 33072 and ISO/IEC 33073. The Transformation process is also being enriched with two other initiatives for creating a PRM and PAM with joint consolidations:
 - a new PRM and PAM is designed and based on the European General Data Protection Regulation (GDPR),
 - another PRM and PAM is designed in the Procurement field, and is based on multiple sources [111].
 - Strengthen the overall TIPA approach by considering underpinning theories such as the Unified process, as explained by Scott [112].
 - Supports the works on Process risk determination (PRD) [C10] in the context of the new GDPR PRM and PAM in particular for the Data Protection Impact Assessment where risk management principles are embedded: process descriptions of the IRMIS PAM for specific risk management processes can help structuring the PRD methodological approach, as well as providing inputs at the ISO level for the upcoming standard ISO/IEC 33015 Information technology – Process assessment - Guide to process risk determination, for a better alignment with ISO 31000.

6. Annex - Terminology tables

The main definitions of concepts used in this PhD thesis are summarized in the various following tables.

	Definition of "Risk"	Selected definition
ISO 31000	<p><i>effect of uncertainty on objectives</i></p> <p>Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.</p> <p>Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.</p> <p>Note 3 to entry: Risk is usually expressed in terms of <i>risk sources</i>, <i>potential events</i>, their <i>consequences</i> and their <i>likelihood</i>.</p>	X
ISO Guide 73	<i>effect of uncertainty on objectives</i>	
Annex SL	<i>effect of uncertainty</i>	
ISO 9000:2015	<i>effect of uncertainty on an expected result</i>	
ISO 21500	-	
ISO/IEC 20000-10	<i>effect of uncertainty</i>	
ISO/IEC 27000	<i>effect of uncertainty on objectives</i>	

	Definition of "Risk management"	Selected definition
ISO 31000	<i>coordinated activities to direct and control an organization with regard to risk</i>	X
ISO Guide 73	<i>coordinated activities to direct and control an organization with regard to risk</i>	
Annex SL	-	
ISO 9000	-	
ISO 21500	-	
ISO/IEC 20000-10	-	

ISO/IEC 27000	<i>coordinated activities to direct and control an organization with regard to risk</i>	
---------------	---	--

	Definition of "Context"	Selected definition
ISO 31000	-	
ISO Guide 73	<i>environment in which the organization seeks to achieve its objectives</i>	X
Annex SL	-	
ISO 9000	<i>business environment; combination of internal and external factors and conditions that can have an effect on an organization's</i>	
ISO 21500	clause on "project environment" stating that "factors outside and inside the organization boundary may impact the project performance"	
ISO/IEC 20000-10	-	
ISO/IEC 27000	-	

	Definition of "Communication and consultation"	Selected definition
ISO 31000	-	
ISO Guide 73	<i>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</i>	X
Annex SL	-	
ISO 9000	Communication fundamental principle: "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."	
ISO 21500	-	
ISO/IEC 20000-10	-	
ISO/IEC 27000	<i>risk communication and consultation</i>	

	<i>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</i>	
--	--	--

	Definition of "Monitoring"	Selected definition
ISO 31000	-	
ISO Guide 73	<i>continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected</i>	X
Annex SL	<i>determining the status of a system, a process or an activity</i>	
ISO 9000	<i>determining the status of a system, a process or an activity</i>	
ISO 21500	-	
ISO/IEC 20000-10	<i>determining the status of a system, a process or an activity</i>	
ISO/IEC 27000	<i>determining the status of a system, a process or an activity</i>	

	Definition of "Review"	Selected definition
ISO 31000	-	
ISO Guide 73	<i>activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives</i>	X
Annex SL		
ISO 9000	<i>determination of the suitability, adequacy or effectiveness of an object to achieve established objectives</i>	
ISO 21500	-	
ISO/IEC 20000-10	-	
ISO/IEC 27000	<i>activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives</i>	

	Definition of “Risk assessment”	Selected definition
ISO 31000	-	
ISO Guide 73	<i>overall process of risk identification, risk analysis and risk evaluation</i>	X
Annex SL	-	
ISO 9000	-	
ISO 21500	-	
ISO/IEC 20000-10	-	
ISO/IEC 27000	<i>overall process of risk identification, risk analysis and risk evaluation</i>	

	Definition of “Risk identification”	Selected definition
ISO 31000	-	
ISO Guide 73	<i>process of finding, recognizing and describing risks</i>	X
Annex SL	-	
ISO 9000	-	
ISO 21500	the purpose of Identify risks process is <i>“to determine potential risk events and their characteristics that, if they occur, may have a positive or negative impact on the project objectives</i>	
ISO/IEC 20000-10	-	
ISO/IEC 27000	<i>process of finding, recognizing and describing risks</i>	

	Definition of “Risk analysis”	Selected definition
ISO 31000	-	
ISO Guide 73	<i>process to comprehend the nature of risk and to determine the level of risk</i>	X
Annex SL	-	

ISO 9000	-	
ISO 21500	-	
ISO/IEC 20000-10	-	
ISO/IEC 27000	<i>process to comprehend the nature of risk and to determine the level of risk</i>	

	Definition of "Risk evaluation"	Selected definition
ISO 31000	-	
ISO Guide 73	<i>process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable</i>	X
Annex SL	-	
ISO 9000	-	
ISO 21500	the purpose of Assess risks process is <i>"to measure and prioritize the risks for further action"</i> .	
ISO/IEC 20000-10	-	
ISO/IEC 27000	<i>process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable</i>	

	Definition of "Risk treatment"	Selected definition
ISO 31000	-	
ISO Guide 73	<i>process to modify risk</i> Note 1 to entry: Risk treatment can involve: — avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; — taking or increasing risk in order to pursue an opportunity; — removing the risk source;	X

	<ul style="list-style-type: none"> — changing the likelihood; — changing the consequences; — sharing the risk with another party or parties (including contracts and risk financing); and — retaining the risk by informed choice. <p>Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.</p> <p>Note 3 to entry: Risk treatment can create new risks or modify existing risks.</p>	
Annex SL	-	
ISO 9000	-	
ISO 21500	the purpose of Treat risks process is “ <i>to develop options and determine actions to enhance opportunities and reduce threats to project objectives</i> ”	
ISO/IEC 20000-10	-	
ISO/IEC 27000	<i>process to modify risk</i>	

	Definition of “Remaining risk”	Selected definition
ISO 31000	No definition but use of “remaining risk” in ISO 31000, instead of residual risk (residual risk is defined in ISO Guide 73)	
ISO Guide 73	<p><i>residual risk</i></p> <p>risk remaining after risk treatment</p> <p>NOTE 1 Residual risk can contain unidentified risk.</p> <p>NOTE 2 Residual risk can also be known as “retained risk”.</p>	
Annex SL	-	
ISO 9000	-	
ISO 21500	-	
ISO/IEC 20000-10	-	

ISO/IEC 27000	<i>residual risk</i> <i>risk remaining after risk treatment</i>	
---------------	--	--

	Definition of “Consequence”	Selected definition
ISO 31000	<i>Outcome of an event affecting objectives</i> Note 1 to entry: A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives. Note 2 to entry: Consequences can be expressed qualitatively or quantitatively. Note 3 to entry: Any consequence can escalate through cascading and cumulative effects.	X
ISO Guide 73	Outcome of an event affecting objectives	
Annex SL	-	
ISO 9000	-	
ISO 21500	-	
ISO/IEC 20000-10	-	
ISO/IEC 27000	-	

7. Annex – Elementary statements from ISO 31000:2018

Main topic	Clause	Clause Title	Text
5 Framework			
5.1 General	5.1	General	The purpose of the risk management framework is to assist the organization in integrating risk management into all its activities and functions.
5.1 General	5.1	General	The effectiveness of risk management will depend on its integration into the governance and all activities of the organization, including decision-making.
5.1 General	5.1	General	This requires support from stakeholders, particularly top management.
5.1 General	5.1	General	Framework development encompasses integrating, designing, implementing, evaluating and improving risk management across the organization.
5.1 General	5.1	General	Figure 3 illustrates the relationship between the components of a framework.
5.1 General	5.1	General	The organization should evaluate its existing risk management practices and processes within the framework.
5.1 General	5.1	General	The organization should evaluate any gaps within the framework.
5.1 General	5.1	General	The organization should address those gaps within the framework.
5.1 General	5.1	General	The components of the framework should be customized to the needs of the organization.
5.1 General	5.1	General	The way in which the components of the framework work together should be customized to the needs of the organization.
5.2 Leadership and commitment	5.2.1	General	Top management and oversight bodies, where applicable, should ensure that risk management is integrated into all organizational activities
5.2 Leadership and commitment	5.2.1	General	Top management and oversight bodies, where applicable, should demonstrate leadership and commitment by aligning risk management with the strategy, objectives and culture of the organization;
5.2 Leadership and commitment	5.2.1	General	Top management and oversight bodies, where applicable, should demonstrate leadership and commitment by issuing a statement or policy that establishes a risk management approach, plan or course of action;
5.2 Leadership and commitment	5.2.1	General	Top management and oversight bodies, where applicable, should demonstrate leadership and commitment by ensuring that the necessary resources are allocated to managing risk;
5.2 Leadership and commitment	5.2.1	General	Top management and oversight bodies, where applicable, should demonstrate leadership and commitment by assigning authority, responsibility and accountability at appropriate levels within the organization;
5.2 Leadership and commitment	5.2.1	General	Top management and oversight bodies, where applicable, should demonstrate leadership and commitment by recognizing and addressing all obligations of the organization, as well as its voluntary commitments;
5.2 Leadership and commitment	5.2.1	General	Top management and oversight bodies, where applicable, should demonstrate leadership and commitment by establishing the amount and type of risk that may or may not be taken by the organization to guide the development of criteria, ensuring that they are communicated to the organization and its stakeholders.
5.2 Leadership and commitment	5.2.1	General	Top management and oversight bodies, where applicable, should demonstrate leadership and commitment by communicating the value of risk management to the organization and its stakeholders;

Main topic	Clause	Clause Title	Text
5.2 Leadership and commitment	5.2.1	General	Top management and oversight bodies, where applicable, should demonstrate leadership and commitment by promoting systematic monitoring of risks;
5.2 Leadership and commitment	5.2.1	General	Top management and oversight bodies, where applicable, should demonstrate leadership and commitment by ensuring that the risk management framework remains appropriate.
5.2 Leadership and commitment	5.2.1	General	Top management is accountable for managing risk while oversight bodies are accountable for overseeing risk management.
5.2 Leadership and commitment	5.2.1	General	Oversight bodies are often expected or required to ensure that risks are adequately considered when setting the organization's objectives;
5.2 Leadership and commitment	5.2.1	General	Oversight bodies are often expected or required to understand the principal risks facing the organization in pursuit of its objectives;
5.2 Leadership and commitment	5.2.1	General	Oversight bodies are often expected or required to ensure that systems to manage such risks are implemented and operating effectively;
5.2 Leadership and commitment	5.2.1	General	Oversight bodies are often expected or required to ensure that such risks are appropriate in the context of the organization's objectives;
5.2 Leadership and commitment	5.2.1	General	Oversight bodies are often expected or required to ensure that information about such risks and their management is properly communicated.
5.2 Leadership and commitment	5.2.2	Integrating risk management	Integrating risk management relies on an understanding of organizational structures and context.
5.2 Leadership and commitment	5.2.2	Integrating risk management	Structures differ depending on the organization's purpose, goals and complexity.
5.2 Leadership and commitment	5.2.2	Integrating risk management	Risk is managed in every part of the organization's structure.
5.2 Leadership and commitment	5.2.2	Integrating risk management	Everyone in the organization has responsibility for managing risk.
5.2 Leadership and commitment	5.2.2	Integrating risk management	Governance guides the course of the organization, its external and internal relationships, and the rules, processes and practices to achieve its purpose.
5.2 Leadership and commitment	5.2.2	Integrating risk management	Management structures translate governance direction into the strategy and associated objectives required to achieve desired levels of sustainable performance and long term viability.
5.2 Leadership and commitment	5.2.2	Integrating risk management	Determining the accountability and oversight roles within an organization are integral parts of the organization's governance.
5.2 Leadership and commitment	5.2.2	Integrating risk management	Integrating risk management into an organization is a dynamic and iterative process,
5.2 Leadership and commitment	5.2.2	Integrating risk management	Integrating risk management into an organization should be customized to the organization's needs and culture.
5.2 Leadership and commitment	5.2.2	Integrating risk management	Risk management should be a part of, and not separate from, the organizational purpose, governance, leadership and commitment, strategy, objectives and operations.
5.3 Design	5.3.1	Understanding the organization and its context	When designing the framework for managing risk, the organization should examine its external and internal context.
5.3 Design	5.3.1	Understanding the organization and its context	When designing the framework for managing risk, the organization should understand its external and internal context.

Main topic	Clause	Clause Title	Text
5.3 Design	5.3.1	Understanding the organization and its context	Examining the organization's external context may include, but is not limited to the social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local;
5.3 Design	5.3.1	Understanding the organization and its context	Examining the organization's external context may include, but is not limited to key drivers and trends affecting the objectives of the organization;
5.3 Design	5.3.1	Understanding the organization and its context	Examining the organization's external context may include, but is not limited to external stakeholders' relationships, perceptions, values, needs and expectations;
5.3 Design	5.3.1	Understanding the organization and its context	Examining the organization's external context may include, but is not limited to contractual relationships and commitments;
5.3 Design	5.3.1	Understanding the organization and its context	Examining the organization's external context may include, but is not limited to the complexity of networks and dependencies.
5.3 Design	5.3.1	Understanding the organization and its context	Examining the organization's internal context may include, but is not limited to vision, mission and values;
5.3 Design	5.3.1	Understanding the organization and its context	Examining the organization's internal context may include, but is not limited to governance, organizational structure, roles and accountabilities;
5.3 Design	5.3.1	Understanding the organization and its context	Examining the organization's internal context may include, but is not limited to strategy, objectives and policies;
5.3 Design	5.3.1	Understanding the organization and its context	Examining the organization's internal context may include, but is not limited to organization's culture;
5.3 Design	5.3.1	Understanding the organization and its context	Examining the organization's internal context may include, but is not limited to standards, guidelines and models adopted by the organization;
5.3 Design	5.3.1	Understanding the organization and its context	Examining the organization's internal context may include, but is not limited to capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, intellectual property, processes, systems and technologies);
5.3 Design	5.3.1	Understanding the organization and its context	Examining the organization's internal context may include, but is not limited to data, information systems and information flows;
5.3 Design	5.3.1	Understanding the organization and its context	Examining the organization's internal context may include, but is not limited to relationships with internal stakeholders, taking into account their perceptions and values;
5.3 Design	5.3.1	Understanding the organization and its context	Examining the organization's internal context may include, but is not limited to contractual relationships and commitments;

Main topic	Clause	Clause Title	Text
5.3 Design	5.3.1	Understanding the organization and its context	Examining the organization's internal context may include, but is not limited to interdependencies and interconnections.
5.3 Design	5.3.2	Articulating risk management commitment	Top management and oversight bodies, where applicable, should articulate their continual commitment to risk management.
5.3 Design	5.3.2	Articulating risk management commitment	Top management and oversight bodies, where applicable, should demonstrate their continual commitment to risk management.
5.3 Design	5.3.2	Articulating risk management commitment	This can be through a policy, a statement or other forms that clearly convey an organization's objectives and commitment to risk management.
5.3 Design	5.3.2	Articulating risk management commitment	The commitment should include, but is not limited to the organization's purpose for managing risk and links to the organization's objectives and other policies;
5.3 Design	5.3.2	Articulating risk management commitment	The commitment should include, but is not limited to reinforcing the need to integrate risk management into the overall culture of the organization;
5.3 Design	5.3.2	Articulating risk management commitment	The commitment should include, but is not limited to leading the integration of risk management into core business activities and decision-making;
5.3 Design	5.3.2	Articulating risk management commitment	The commitment should include, but is not limited to authorities, responsibilities and accountabilities;
5.3 Design	5.3.2	Articulating risk management commitment	The commitment should include, but is not limited to making the necessary resources available;
5.3 Design	5.3.2	Articulating risk management commitment	The commitment should include, but is not limited to the way in which conflicting objectives are dealt with;
5.3 Design	5.3.2	Articulating risk management commitment	The commitment should include, but is not limited to measurement and reporting within the organization's performance indicators;
5.3 Design	5.3.2	Articulating risk management commitment	The commitment should include, but is not limited to review and improvement.
5.3 Design	5.3.2	Articulating risk management commitment	The risk management commitment should be communicated within an organization and to stakeholders, as appropriate.
5.3 Design	5.3.3	Assigning organizational roles, authorities, responsibilities and accountabilities	Top management and oversight bodies, where applicable, should ensure that the accountabilities, responsibilities and authorities for relevant roles with respect to risk management are assigned
5.3 Design	5.3.3	Assigning organizational roles, authorities, responsibilities and accountabilities	Top management and oversight bodies, where applicable, should ensure that the accountabilities, responsibilities and authorities for relevant roles with respect to risk management are communicated at all levels of the organization

Main topic	Clause	Clause Title	Text
5.3 Design	5.3.3	Assigning organizational roles, authorities, responsibilities and accountabilities	Top management and oversight bodies, where applicable, should ensure that the accountabilities, responsibilities and authorities for relevant roles with respect to risk management should emphasise that risk management is a core responsibility;
5.3 Design	5.3.3	Assigning organizational roles, authorities, responsibilities and accountabilities	Top management and oversight bodies, where applicable, should ensure that the accountabilities, responsibilities and authorities for relevant roles with respect to risk management should identify individuals who have the accountability and authority to manage risk (risk owners).
5.3 Design	5.3.4	Allocating resources	Top management and oversight bodies, where applicable, should ensure allocation of appropriate resources for risk management,
5.3 Design	5.3.4	Allocating resources	Top management and oversight bodies, where applicable, should ensure allocation of appropriate resources for risk management, which can include, but are not limited to people, skills, experience and competence;
5.3 Design	5.3.4	Allocating resources	Top management and oversight bodies, where applicable, should ensure allocation of appropriate resources for risk management, which can include, but are not limited to the organization's processes, methods and tools to be used for managing risk;
5.3 Design	5.3.4	Allocating resources	Top management and oversight bodies, where applicable, should ensure allocation of appropriate resources for risk management, which can include, but are not limited to documented processes and procedures;
5.3 Design	5.3.4	Allocating resources	Top management and oversight bodies, where applicable, should ensure allocation of appropriate resources for risk management, which can include, but are not limited to information and knowledge management systems;
5.3 Design	5.3.4	Allocating resources	Top management and oversight bodies, where applicable, should ensure allocation of appropriate resources for risk management, which can include, but are not limited to professional development and training needs.
5.3 Design	5.3.4	Allocating resources	The organization should consider the capabilities of, and constraints on, existing resources.
5.3 Design	5.3.5	Establishing communication and consultation	The organization should establish an agreed approach to communication and consultation to support the framework
5.3 Design	5.3.5	Establishing communication and consultation	The organization should establish an agreed approach to communication and consultation to facilitate the effective application of risk management.
5.3 Design	5.3.5	Establishing communication and consultation	Communication involves sharing information with targeted audiences, where consultation also involves participants providing feedback with the expectation that it will contribute to and shape decisions or other activities.
5.3 Design	5.3.5	Establishing communication and consultation	Communication and consultation methods and content should reflect the expectations of stakeholders, where relevant.

Main topic	Clause	Clause Title	Text
5.3 Design	5.3.5	Establishing communication and consultation	Communication and consultation should be timely
5.3 Design	5.3.5	Establishing communication and consultation	Communication and consultation should ensure that relevant information is captured, consolidated and shared, as appropriate
5.3 Design	5.3.5	Establishing communication and consultation	Communication and consultation should ensure that feedback is provided and improvements are made.
5.4 Implementation	5.4	Implementation	The organization should implement the risk management framework by developing an appropriate plan including timing;
5.4 Implementation	5.4	Implementation	The organization should implement the risk management framework by identifying where, when and how different types of decisions are made across the organization, and by whom;
5.4 Implementation	5.4	Implementation	The organization should implement the risk management framework by modifying the applicable decision-making processes where necessary;
5.4 Implementation	5.4	Implementation	The organization should implement the risk management framework by ensuring that the organization's arrangements for managing risk are clearly understood and practised.
5.4 Implementation	5.4	Implementation	Successful implementation of the framework requires the engagement and awareness of stakeholders.
5.4 Implementation	5.4	Implementation	This enables organizations to explicitly address uncertainty in decision-making, while also ensuring that any new or subsequent uncertainty can be taken into account as it arises.
5.4 Implementation	5.4	Implementation	Properly designed and implemented, the risk management framework will ensure that the risk management process is a part of all activities throughout the organization, including decision-making
5.4 Implementation	5.4	Implementation	Properly designed and implemented, the risk management framework will ensure that changes in external and internal contexts will be adequately captured.
5.5 Evaluation	5.4	Implementation	In order to evaluate the effectiveness of the risk management framework, the organization should periodically measure risk management framework performance against its purpose, implementation plans, indicators and expected behaviour;
5.5 Evaluation	5.4	Implementation	In order to evaluate the effectiveness of the risk management framework, the organization should determine whether it remains suitable to support achieving the objectives of the organization.
5.6 Improvement	5.6.1	Adapting	The organization should continually monitor the risk management framework to address external and internal changes.
5.6 Improvement	5.6.1	Adapting	The organization should continually adapt the risk management framework to address external and internal changes.
5.6 Improvement	5.6.1	Adapting	In doing so, the organization can improve its value.
5.6 Improvement	5.6.2	Continually improving	The organization should continually improve the suitability, adequacy and effectiveness of the risk management framework
5.6 Improvement	5.6.2	Continually improving	The organization should continually improve the way the risk management process is integrated.

Main topic	Clause	Clause Title	Text
5.6 Improvement	5.6.2	Continually improving	As relevant gaps or improvement opportunities are identified, the organization should develop plans and tasks
5.6 Improvement	5.6.2	Continually improving	As relevant gaps or improvement opportunities are identified, the organization should assign plans and tasks to those accountable for implementation.
5.6 Improvement	5.6.2	Continually improving	Once implemented, these improvements should contribute to the enhancement of risk management.
6 Process			
6.1 General	6.1	General	The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.
6.1 General	6.1	General	The risk management process should be an integral part of management and decision-making
6.1 General	6.1	General	The risk management process should be integrated into the structure, operations and processes of the organization.
6.1 General	6.1	General	It can be applied at strategic, operational, programme or project levels.
6.1 General	6.1	General	There can be many applications of the risk management process within an organization, customized to achieve objectives and to suit the external and internal context in which they are applied.
6.1 General	6.1	General	The dynamic and variable nature of human behaviour and culture should be considered throughout the risk management process.
6.1 General	6.1	General	Although the risk management process is often presented as sequential, in practice it is iterative.
6.2 Communication and consultation	6.2	Communication and consultation	The purpose of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required.
6.2 Communication and consultation	6.2	Communication and consultation	Communication seeks to promote awareness and understanding of risk and how to deal with it, whereas consultation involves obtaining feedback and information to support decision-making.
6.2 Communication and consultation	6.2	Communication and consultation	Close coordination between the two should facilitate factual, timely, relevant, accurate and understandable exchanges of information, taking into account the confidentiality and integrity of information as well as the privacy rights of individuals.
6.2 Communication and consultation	6.2	Communication and consultation	Communication and consultation with appropriate external and internal stakeholders should take place within and throughout all steps of the risk management process.
6.2 Communication and consultation	6.2	Communication and consultation	Communication and consultation aims to bring different areas of expertise together for each step of the risk management process;
6.2 Communication and consultation	6.2	Communication and consultation	Communication and consultation aims to ensure that different views are appropriately considered when defining risk criteria and when evaluating risks;
6.2 Communication and consultation	6.2	Communication and consultation	Communication and consultation aims to provide sufficient information to facilitate risk oversight and decision-making;;
6.2 Communication and consultation	6.2	Communication and consultation	Communication and consultation aims to build a sense of inclusiveness and ownership among those affected by risk.

Main topic	Clause	Clause Title	Text
6.3 Establishing the context	6.3.1	General	The purpose of establishing the context is to customise the risk management process, enabling effective risk assessment and appropriate risk treatment.
6.3 Establishing the context	6.3.1	General	To customise the risk management process involves defining the purpose and scope of the process.
6.3 Establishing the context	6.3.1	General	To customise the risk management process involves understanding the context.
6.3 Establishing the context	6.3.1	General	To customise the risk management process involves planning the approach to be taken.
6.3 Establishing the context	6.3.1	General	To customise the risk management process involves defining the criteria for evaluation.
6.3 Establishing the context	6.3.1	General	Establishing the context should take into account the external and internal context established as part of the risk management framework.
6.3 Establishing the context	6.3.2	Defining the purpose and scope	The organization should define the purpose and scope of its risk management activities.
6.3 Establishing the context	6.3.2	Defining the purpose and scope	As the risk management process may be applied at different levels (e.g. strategic, operational, programme, project, or other activities), it is important to be clear about the scope under consideration, the relevant objectives to be considered and their alignment with organizational objectives.
6.3 Establishing the context	6.3.2	Defining the purpose and scope	When planning the approach, considerations include objectives and decisions that need to be made
6.3 Establishing the context	6.3.2	Defining the purpose and scope	When planning the approach, considerations include outcomes expected from the steps to be taken in the process
6.3 Establishing the context	6.3.2	Defining the purpose and scope	When planning the approach, considerations include time, location, specific inclusions and exclusions
6.3 Establishing the context	6.3.2	Defining the purpose and scope	When planning the approach, considerations include appropriate risk assessment tools and techniques
6.3 Establishing the context	6.3.2	Defining the purpose and scope	When planning the approach, considerations include resources required, responsibilities and records to be kept
6.3 Establishing the context	6.3.2	Defining the purpose and scope	When planning the approach, considerations include relationships with other projects, processes and activities.
6.3 Establishing the context	6.3.3	Context	The external and internal context is the environment in which the organization seeks to define and achieve its objectives.
6.3 Establishing the context	6.3.3	Context	The context of the risk management process should be derived from the understanding of the external and internal environment in which the organization operates
6.3 Establishing the context	6.3.3	Context	The context of the risk management process should reflect the specific environment of the activity to which the risk management process is to be applied.
6.3 Establishing the context	6.3.3	Context	Understanding the context is important because risk management takes place in the context of the objectives and activities of the organization
6.3 Establishing the context	6.3.3	Context	Understanding the context is important because organizational factors can be a source of risk;

Main topic	Clause	Clause Title	Text
6.3 Establishing the context	6.3.3	Context	Understanding the context is important because the purpose and scope of where the risk management process is being applied can be interrelated with the objectives of the organization as a whole;
6.3 Establishing the context	6.3.3	Context	Understanding the context is important because the organization should establish the external and internal context of the risk management process by considering the factors mentioned in 5.3.1.
6.3 Establishing the context	6.3.4	Defining risk criteria	The organization should specify the amount and type of risk that it may or may not take, relative to objectives.
6.3 Establishing the context	6.3.4	Defining risk criteria	It should also define criteria to evaluate the significance of risk.
6.3 Establishing the context	6.3.4	Defining risk criteria	It should also define criteria to support decision-making processes.
6.3 Establishing the context	6.3.4	Defining risk criteria	Risk criteria should be aligned with the risk management framework.
6.3 Establishing the context	6.3.4	Defining risk criteria	Risk criteria should be customized to the specific purpose and scope of the activity under consideration.
6.3 Establishing the context	6.3.4	Defining risk criteria	Risk criteria should reflect the organization's values, objectives and resources.
6.3 Establishing the context	6.3.4	Defining risk criteria	Risk criteria should be consistent with policies and statements about risk management.
6.3 Establishing the context	6.3.4	Defining risk criteria	The criteria should be defined taking into consideration the organization's obligations and the views of stakeholders.
6.3 Establishing the context	6.3.4	Defining risk criteria	While risk criteria should be established at the beginning of the risk assessment process, they are dynamic and should be continually reviewed, if necessary.
6.3 Establishing the context	6.3.4	Defining risk criteria	While risk criteria should be established at the beginning of the risk assessment process, they are dynamic and should be continually amended, if necessary.
6.3 Establishing the context	6.3.4	Defining risk criteria	To set risk criteria, the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible) should be considered
6.3 Establishing the context	6.3.4	Defining risk criteria	To set risk criteria, how consequences (both positive and negative) will be defined and measured should be considered
6.3 Establishing the context	6.3.4	Defining risk criteria	To set risk criteria, how likelihood will be defined and measured should be considered
6.3 Establishing the context	6.3.4	Defining risk criteria	To set risk criteria, time-related factors should be considered
6.3 Establishing the context	6.3.4	Defining risk criteria	To set risk criteria, consistency in the use of measurements should be considered
6.3 Establishing the context	6.3.4	Defining risk criteria	To set risk criteria, how the level of risk is to be determined should be considered
6.3 Establishing the context	6.3.4	Defining risk criteria	To set risk criteria, how combinations and sequences of multiple risks will be taken into account should be considered
6.3 Establishing the context	6.3.4	Defining risk criteria	To set risk criteria, the organization's capacity should be considered
6.4 Risk assessment	6.4.1	General	Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.
6.4 Risk assessment	6.4.1	General	Risk assessment should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders.
6.4 Risk assessment	6.4.1	General	Risk assessment should use the best available information, supplemented by further enquiry as necessary.

Main topic	Clause	Clause Title	Text
6.4 Risk assessment	6.4.2	Risk identification	The purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization from achieving its objectives.
6.4 Risk assessment	6.4.2	Risk identification	Relevant, appropriate and up-to-date information is important in identifying risks.
6.4 Risk assessment	6.4.2	Risk identification	The organization can use a range of techniques to identify uncertainties that might affect one or more objectives.
6.4 Risk assessment	6.4.2	Risk identification	<i>A set of</i> factors, and the relationship between these factors, should be considered
6.4 Risk assessment	6.4.2	Risk identification	Tangible and intangible sources of risk (<i>factor</i>) should be considered
6.4 Risk assessment	6.4.2	Risk identification	Causes and events (<i>factor</i>) should be considered
6.4 Risk assessment	6.4.2	Risk identification	Threats and opportunities (<i>factor</i>) should be considered
6.4 Risk assessment	6.4.2	Risk identification	Vulnerabilities and capabilities (<i>factor</i>) should be considered
6.4 Risk assessment	6.4.2	Risk identification	Changes in the external and internal context (<i>factor</i>) should be considered
6.4 Risk assessment	6.4.2	Risk identification	Indicators of emerging risks (<i>factor</i>) should be considered
6.4 Risk assessment	6.4.2	Risk identification	The nature and value of assets and resources (<i>factor</i>) should be considered
6.4 Risk assessment	6.4.2	Risk identification	Consequences and their impact on objectives (<i>factor</i>) should be considered
6.4 Risk assessment	6.4.2	Risk identification	Limitations of knowledge and reliability of information (<i>factor</i>) should be considered
6.4 Risk assessment	6.4.2	Risk identification	Timeframes and time influences (<i>factor</i>) should be considered
6.4 Risk assessment	6.4.2	Risk identification	Biases, assumptions and beliefs of those involved (<i>factor</i>) should be considered
6.4 Risk assessment	6.4.2	Risk identification	The organization should identify risks, whether or not their sources are under its control
6.4 Risk assessment	6.4.2	Risk identification	Consideration should be given that there might be more than one type of outcome, which might result in a variety of tangible or intangible consequences.
6.4 Risk assessment	6.4.3	Risk analysis	The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk.
6.4 Risk assessment	6.4.3	Risk analysis	Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness.
6.4 Risk assessment	6.4.3	Risk analysis	An event can have multiple causes and consequences and can affect multiple objectives.
6.4 Risk assessment	6.4.3	Risk analysis	Risk analysis can be undertaken with varying degrees of detail and formality, depending on the purpose of the analysis, the availability and reliability of information, and the resources available.
6.4 Risk assessment	6.4.3	Risk analysis	Analysis techniques can be qualitative, semi quantitative, quantitative or a combination of these, depending on the circumstances and intended use.
6.4 Risk assessment	6.4.3	Risk analysis	Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur
6.4 Risk assessment	6.4.3	Risk analysis	Risk analysis should consider factors such as the likelihood of events and consequences

Main topic	Clause	Clause Title	Text
6.4 Risk assessment	6.4.3	Risk analysis	Risk analysis should consider factors such as the nature and magnitude of consequences
6.4 Risk assessment	6.4.3	Risk analysis	Risk analysis should consider factors such as complexity and connectivity
6.4 Risk assessment	6.4.3	Risk analysis	Risk analysis should consider factors such as time-related factors and volatility
6.4 Risk assessment	6.4.3	Risk analysis	Risk analysis should consider factors such as the pace of change
6.4 Risk assessment	6.4.3	Risk analysis	Risk analysis should consider factors such as the effectiveness of existing controls
6.4 Risk assessment	6.4.3	Risk analysis	Risk analysis should consider factors such as sensitivity and confidence levels
6.4 Risk assessment	6.4.3	Risk analysis	The risk analysis can be influenced by any divergence of opinions, biases, perceptions of risk and judgements.
6.4 Risk assessment	6.4.3	Risk analysis	Additional influences are the quality of the information used, the assumptions and exclusions made, any limitations of the techniques and how they are executed.
6.4 Risk assessment	6.4.3	Risk analysis	These influences should be considered.
6.4 Risk assessment	6.4.3	Risk analysis	These influences should be documented.
6.4 Risk assessment	6.4.3	Risk analysis	These influences should be communicated to decision makers.
6.4 Risk assessment	6.4.3	Risk analysis	Highly uncertain events can be difficult to quantify.
6.4 Risk assessment	6.4.3	Risk analysis	This can be an issue when analysing events with severe consequences.
6.4 Risk assessment	6.4.3	Risk analysis	In such cases, a combination of techniques should provide greater insight overall.
6.4 Risk assessment	6.4.3	Risk analysis	Risk analysis provides an input to risk evaluation.
6.4 Risk assessment	6.4.3	Risk analysis	Risk analysis provides an input to decisions on whether risk needs to be treated and how.
6.4 Risk assessment	6.4.3	Risk analysis	Risk analysis provides an input on the most appropriate risk treatment strategy and methods.
6.4 Risk assessment	6.4.3	Risk analysis	The results provide insight for decisions, where choices are being made, and the options involve different types and levels of risk.
6.4 Risk assessment	6.4.4	Risk evaluation	The purpose of risk evaluation is to support decisions.
6.4 Risk assessment	6.4.4	Risk evaluation	Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine the significance of risk.
6.4 Risk assessment	6.4.4	Risk evaluation	The significance of risk can lead to a decision to do nothing further
6.4 Risk assessment	6.4.4	Risk evaluation	The significance of risk can lead to a decision to consider risk treatment options
6.4 Risk assessment	6.4.4	Risk evaluation	The significance of risk can lead to a decision to undertake further analysis to better understand the risk;
6.4 Risk assessment	6.4.4	Risk evaluation	The significance of risk can lead to a decision to maintain existing controls
6.4 Risk assessment	6.4.4	Risk evaluation	The significance of risk can lead to a decision to reconsider objectives.
6.4 Risk assessment	6.4.4	Risk evaluation	Decisions should take account of the wider context and the actual and perceived consequences for external and internal stakeholders.

Main topic	Clause	Clause Title	Text
6.4 Risk assessment	6.4.4	Risk evaluation	The outcome of risk evaluation should be recorded.
6.4 Risk assessment	6.4.4	Risk evaluation	The outcome of risk evaluation should be communicated.
6.4 Risk assessment	6.4.4	Risk evaluation	The outcome of risk evaluation should be then validated at appropriate levels of the organization.
6.5 Risk treatment	6.5.1	General	The purpose of risk treatment is to select and implement options for addressing risk.
6.5 Risk treatment	6.5.1	General	Risk treatment involves an iterative process of formulating and selecting risk treatment options
6.5 Risk treatment	6.5.1	General	Risk treatment involves an iterative process of planning and implementing risk treatment
6.5 Risk treatment	6.5.1	General	Risk treatment involves an iterative process of assessing the effectiveness of that treatment
6.5 Risk treatment	6.5.1	General	Risk treatment involves an iterative process of deciding whether the residual risk is acceptable
6.5 Risk treatment	6.5.1	General	Risk treatment involves an iterative process of if not acceptable, taking further treatment.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives against the costs, effort, or disadvantages of implementation.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Options for treating risk can involve one or more <i>actions</i>
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Options for treating risk can involve avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Options for treating risk can involve taking or increasing the risk in order to pursue an opportunity
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Options for treating risk can involve removing the risk source
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Options for treating risk can involve changing the likelihood
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Options for treating risk can involve changing the consequences
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Options for treating risk can involve sharing the risk (e.g. through contracts, buying insurance)
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Options for treating risk can involve retaining the risk by informed decision.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Justification for risk treatment is broader than solely economic considerations.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Justification for risk treatment should take into account all of the organization's obligations.

Main topic	Clause	Clause Title	Text
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Justification for risk treatment should take into account all of the voluntary commitments.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Justification for risk treatment should take into account all of the stakeholder views.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	The selection of risk treatment options should be made in accordance with the organization's objectives.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	The selection of risk treatment options should be made in accordance with risk criteria.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	The selection of risk treatment options should be made in accordance with available resources.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	When selecting risk treatment options, the organization should consider the values, perceptions and potential involvement of stakeholders.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	When selecting risk treatment options, the organization should consider the most appropriate ways to communicate and consult with stakeholders.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Though carefully designed and implemented, risk treatment might not produce the expected outcomes and could produce unintended consequences.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Monitoring and review need to be an integral part of the risk treatment implementation to give assurance that the different forms of treatment become and remain effective.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Risk treatment can also introduce new risks that need to be managed.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	If there are no treatment options available or if treatment options do not sufficiently modify the risk, the risk should be recorded.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	If there are no treatment options available or if treatment options do not sufficiently modify the risk, the risk should be kept under ongoing review.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	Decision makers and other stakeholders should be aware of the nature and extent of the residual risk after risk treatment.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	The residual risk should be documented.
6.5 Risk treatment	6.5.2	Selection of risk treatment options	The residual risk should be subjected to monitoring, review and, where appropriate, further treatment.
6.5 Risk treatment	6.5.3	Preparing and implementing risk treatment plans	The purpose of risk treatment plans is to specify how the chosen treatment options will be implemented, so that arrangements are understood by those involved, and progress against the plan can be monitored.
6.5 Risk treatment	6.5.3	Preparing and implementing risk treatment plans	The treatment plan should clearly identify the order in which risk treatment should be implemented.
6.5 Risk treatment	6.5.3	Preparing and implementing	Treatment plans should be integrated into the management plans and processes of the organization, in consultation with appropriate stakeholders.

Main topic	Clause	Clause Title	Text
		risk treatment plans	
6.5 Risk treatment	6.5.3	Preparing and implementing risk treatment plans	The information provided in the treatment plan should include the rationale for selection of the treatment options, including the expected benefits to be gained
6.5 Risk treatment	6.5.3	Preparing and implementing risk treatment plans	The information provided in the treatment plan should include those who are accountable and responsible for approving and implementing the plan
6.5 Risk treatment	6.5.3	Preparing and implementing risk treatment plans	The information provided in the treatment plan should include the proposed actions
6.5 Risk treatment	6.5.3	Preparing and implementing risk treatment plans	The information provided in the treatment plan should include the resources required, including contingencies
6.5 Risk treatment	6.5.3	Preparing and implementing risk treatment plans	The information provided in the treatment plan should include the performance measures
6.5 Risk treatment	6.5.3	Preparing and implementing risk treatment plans	The information provided in the treatment plan should include the constraints
6.5 Risk treatment	6.5.3	Preparing and implementing risk treatment plans	The information provided in the treatment plan should include the required reporting and monitoring
6.5 Risk treatment	6.5.3	Preparing and implementing risk treatment plans	The information provided in the treatment plan should include when actions are expected to be undertaken and completed.
6.6 Monitoring and review	6.6	Monitoring and review	The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes.
6.6 Monitoring and review	6.6	Monitoring and review	Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of the risk management process, with responsibilities clearly defined.
6.6 Monitoring and review	6.6	Monitoring and review	Monitoring and review should take place at all stages of the process.
6.6 Monitoring and review	6.6	Monitoring and review	Monitoring and review includes planning, gathering and analysing information, recording results and providing feedback.
6.6 Monitoring and review	6.6	Monitoring and review	The results of monitoring and review should be incorporated throughout the organization's performance management.
6.6 Monitoring and review	6.6	Monitoring and review	The results of monitoring and review should be incorporated throughout the organization's measurement.
6.6 Monitoring and review	6.6	Monitoring and review	The results of monitoring and review should be incorporated throughout the organization's reporting activities.
6.7 Recording the risk management process	6.7	Recording and reporting	The risk management process and its outcomes should be documented and reported through appropriate mechanisms.

Main topic	Clause	Clause Title	Text
6.7 Recording the risk management process	6.7	Recording and reporting	Recording and reporting communicates risk management activities and outcomes across the organization
6.7 Recording the risk management process	6.7	Recording and reporting	Recording and reporting provides information for decision-making
6.7 Recording the risk management process	6.7	Recording and reporting	Recording and reporting improves risk management activities
6.7 Recording the risk management process	6.7	Recording and reporting	Recording and reporting assists interaction with stakeholders, including those with responsibility and accountability for risk management activities
6.7 Recording the risk management process	6.7	Recording and reporting	Decisions concerning the creation, retention and handling of documented information should take into account, but not be limited to, their use
6.7 Recording the risk management process	6.7	Recording and reporting	Decisions concerning the creation, retention and handling of documented information should take into account, but not be limited to, the sensitivity of information
6.7 Recording the risk management process	6.7	Recording and reporting	Decisions concerning the creation, retention and handling of documented information should take into account, but not be limited to, the external and internal context.
6.7 Recording the risk management process	6.7	Recording and reporting	Reporting is an integral part of organization's governance
6.7 Recording the risk management process	6.7	Recording and reporting	Reporting should enhance the quality of dialogue with stakeholders
6.7 Recording the risk management process	6.7	Recording and reporting	Reporting should support top management and oversight bodies in meeting their responsibilities.
6.7 Recording the risk management process	6.7	Recording and reporting	Factors to consider for reporting include, but are not limited to the differing stakeholders and their specific information needs and requirements
6.7 Recording the risk management process	6.7	Recording and reporting	Factors to consider for reporting include, but are not limited to the cost, frequency and timeliness of reporting
6.7 Recording the risk management process	6.7	Recording and reporting	Factors to consider for reporting include, but are not limited to the method of reporting
6.7 Recording the risk management process	6.7	Recording and reporting	Factors to consider for reporting include, but are not limited to the relevance of information to organizational objectives and decision-making

8. Annex - Requirement trees and goal trees for risk management specific processes

8.1 Requirement tree and goal tree for Risk criteria definition process

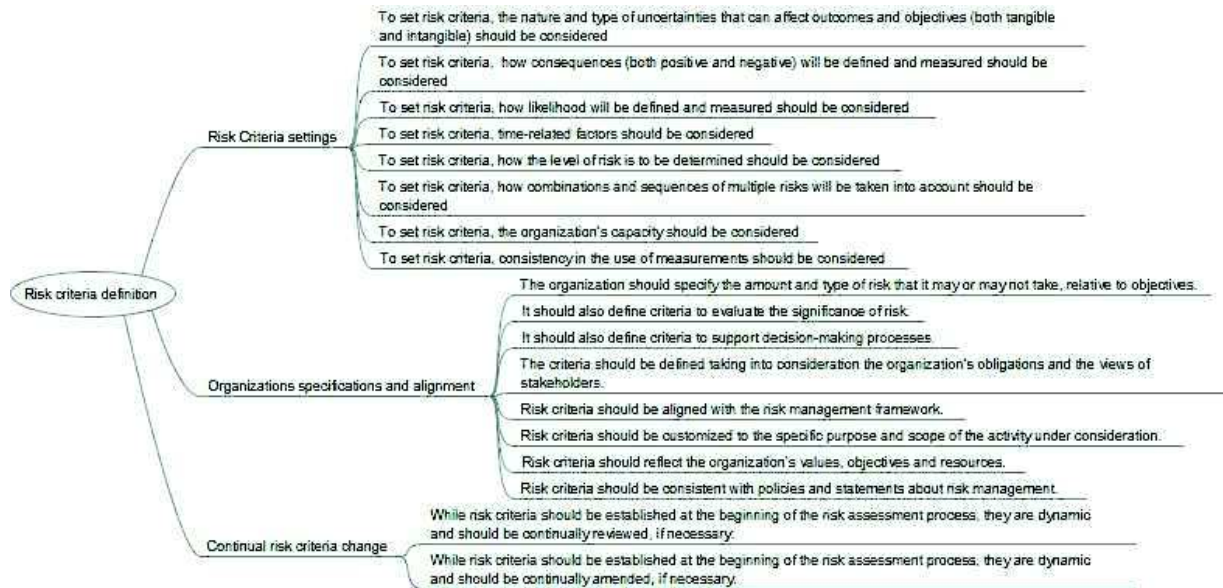


Figure 2: Requirement tree for Risk criteria definition process

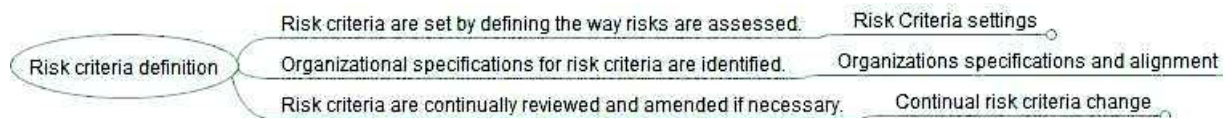


Figure 3: Goal tree for Risk criteria definition process

8.2 Requirement tree and goal tree for Risk identification process

The purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization from achieving its objectives.

The organization can use a range of techniques to identify uncertainties that might affect one or more objectives.

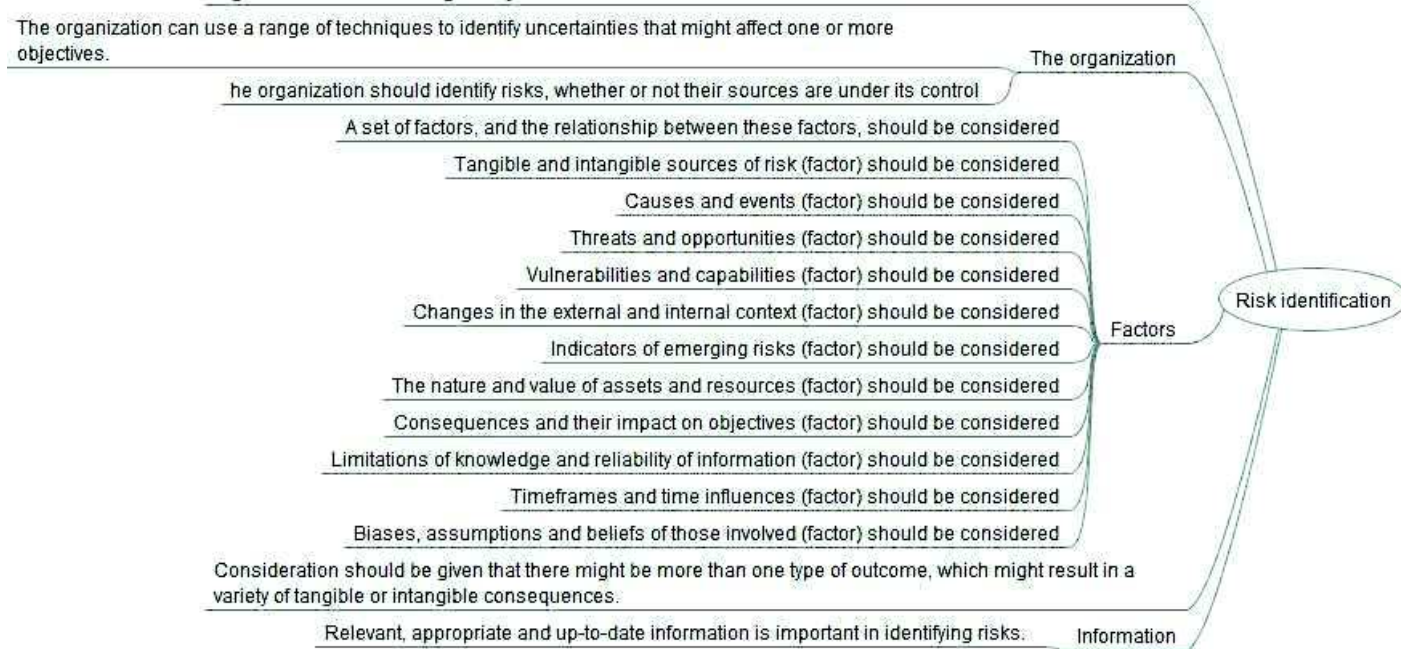


Figure 4: Requirement tree for Risk identification process

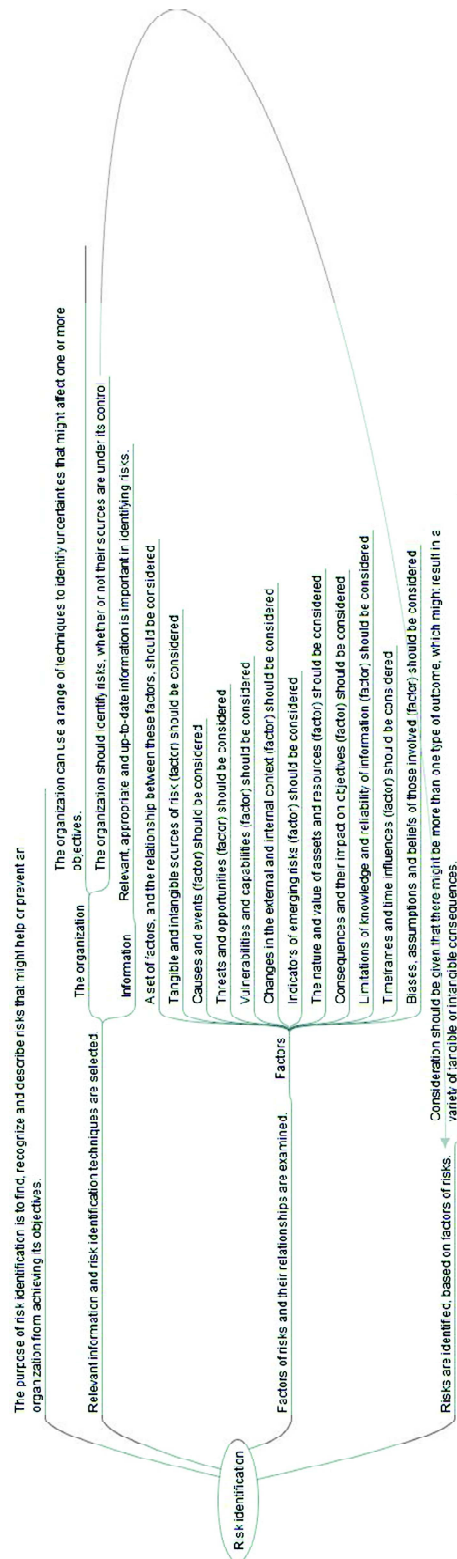


Figure 5: Goal tree for Risk identification process

8.3 Requirement tree and goal tree for Risk analysis process



Figure 6: Requirement tree for Risk analysis process

8.4 Requirement tree and goal tree for Risk evaluation process

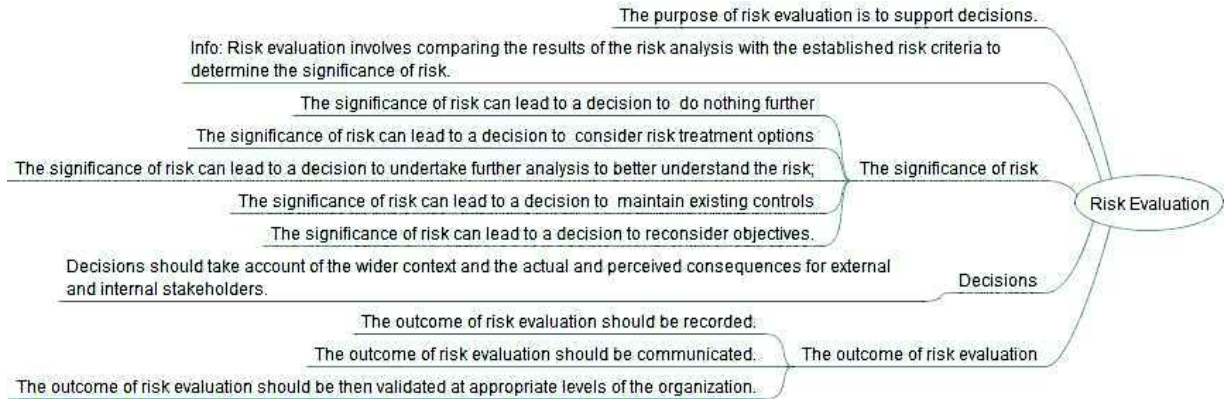


Figure 8: Requirement tree for Risk evaluation process

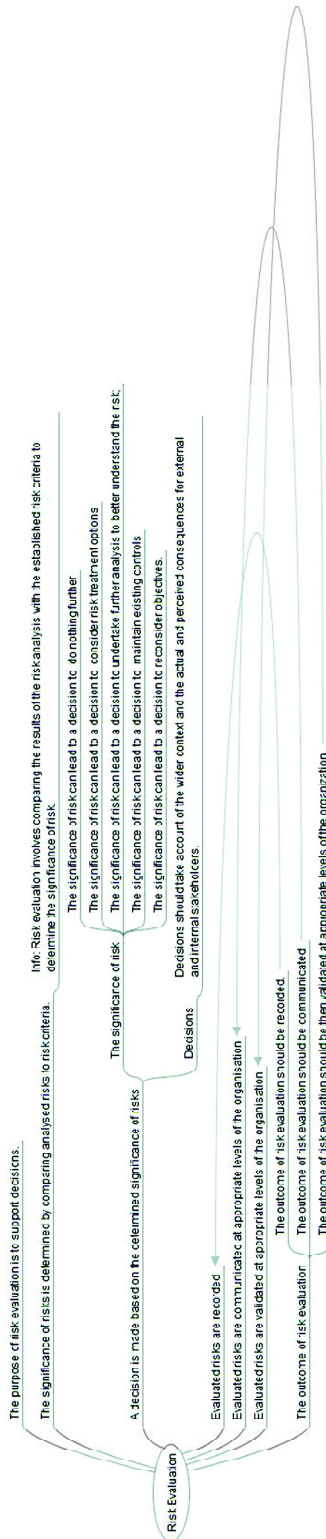


Figure 9: Goal tree for Risk evaluation process

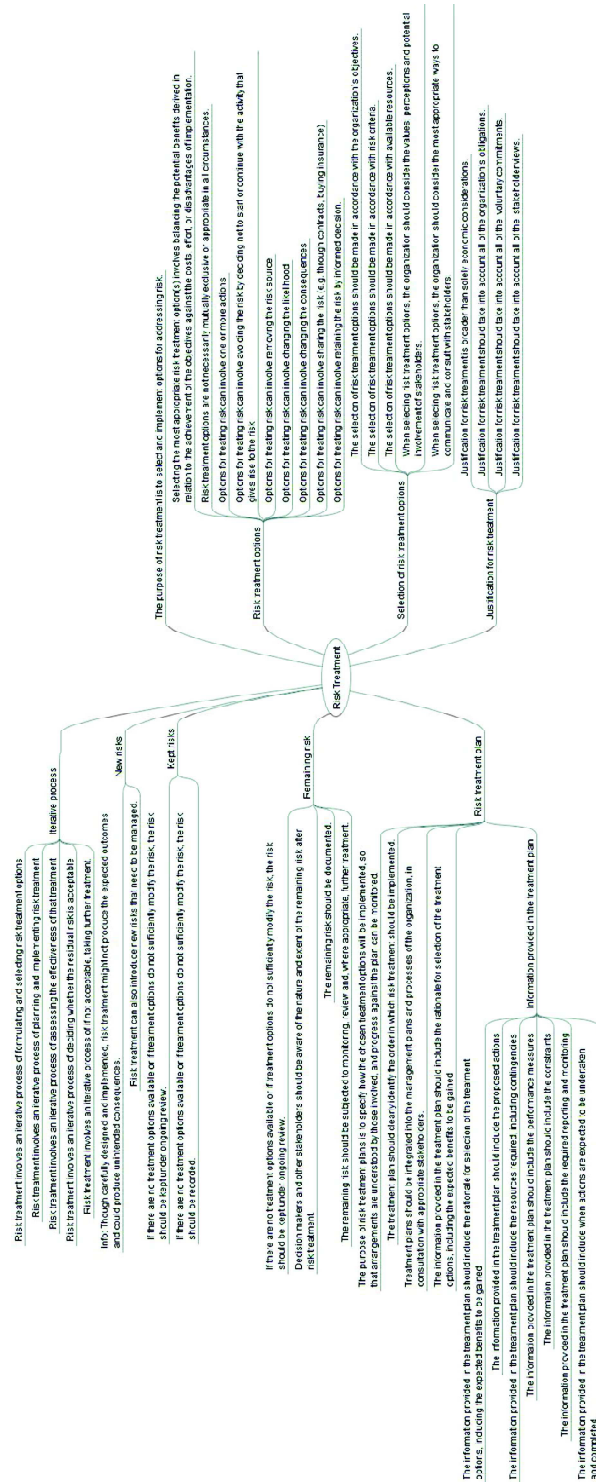


Figure 11: Goal tree for Risk treatment process

9. Annex - IRMIS PAM

9.1 Introduction

This Process Assessment Model (PAM) has been produced by Béatrix Barafort in the context of her PhD studies.

The PAM defined in this document is based on the ISO 31000 International Standard (published in 2018), with an integration approach related to the ISO 9001, ISO 21500, ISO/IEC 20000-1 and ISO/IEC 27001. Views of some of these latter standards are also provided.

9.1.1 Definition of a Process Assessment Model

A Process Assessment Model is related to one or more Process Reference Models. It forms the basis for the collection of evidence and rating of process capability.

A Process Assessment Model provides a two-dimensional view of process maturity.

In the process dimension, it describes a set of processes that relate to the processes defined in the selected Process Reference Model(s). In addition to information provided in the PRM, processes are described with a set of indicators (e.g. base practices and work products).

In the capability dimension, the Process Assessment Model describes capabilities that relate to the process capability levels and process attributes defined in ISO/IEC 33020.

Requirements related to Process Assessment Models are defined in part 6.3 of ISO/IEC 33004.

9.1.2 Foreword

The following writing conventions apply in the below process descriptions:

- [*ref*] refers to a source of information for this PAM element.
- [Outcome x] links this element to a specified Expected Result of the same process.
- [BPx] links this element to a specified base practice of the same process.
- NOTE x Notes are added to PAM elements to clarify their meaning.

9.2 PAM process map



9.3 Description of processes

9.3.1 Top Management Process

9.3.1.1 TOP.01 Leadership

Process ID	TOP.01
Process Name	Leadership <i>[ref]</i>
Comment	Ref ISO/IEC 33073 TOP.01 Note 1: “Quality management system” has been replaced by “risk management framework”; quality policy” has been replaced by “risk management policy”
Process Purpose	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.
Process Outcomes	As a result of successful implementation of the Leadership process: <ol style="list-style-type: none"> 1. The context of the organisation, including the expectations of its relevant interested parties, are understood and analysed; 2. The scope of risk management activities is defined, taking the context of the organisation into consideration; 3. The risk management policy and objectives are defined ; <i>[ref]</i> 4. The risk management framework and operational process strategy is determined; 5. Commitment and leadership with respect to the risk management framework is demonstrated.
Base Practices	TOP.1.BP.1 Determine external and internal issues that are relevant to the organization and analyze their impacts. Determine external and internal issues that are relevant to the purpose of the assessed organization and that affect its ability to achieve the intended outcome(s) of its risk management framework. [Outcome 1] TOP.1.BP.2 Determine the relevant interested parties and analyze their requirements. Determine the relevant interested parties that are relevant to the risk management framework and establish appropriate contacts with them. [Outcome 1]

	<p>TOP.1.BP.3 Determine the scope of the risk management framework. Determine the boundaries and applicability of the risk management framework, taking into consideration the context of the organization, the requirements of relevant interested parties and the interfaces and dependencies between activities performed by the organization, and those that are performed by other organization. [Outcome 2]</p> <p>TOP.1.BP.4 Define a risk management policy. Define a risk management policy that is appropriate to the purpose of the organization. [Outcome 3]</p> <p>TOP.1.BP.5 Define risk management objectives. Define risk management objectives at relevant functions and levels, which are measurable, consistent with the risk management policy. [Outcome 3]</p> <p>TOP.1.BP.6 Determine process strategy. Determine the management framework and operational process strategy. [Outcome 4]</p> <p>TOP.1.BP.7 Integrate the risk management framework requirements into the business processes of the organization. Ensure the integration of the risk management framework requirements into the business processes of the organization. [Outcome 5]</p> <p>TOP.1.BP.8 Demonstrate leadership by enabling contributions to organizational effectiveness. Direct and support persons to contribute to the effectiveness of the risk management framework and support other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility. [Outcome 5]</p>
--	---

9.3.2 Common Processes

9.3.2.1 COM.01 Communication management

Process ID	COM.01
Process Name	Communication management <i>[ref]</i>
Comment	Ref ISO/IEC 33073 COM.01 In ISO 31000, the purpose of communication and consultation is “to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required”.
Process Purpose	The purpose of Communication management is to produce timely and accurate information products to support effective communication and decision making.
Process Outcomes	As a result of successful implementation of the Communication management process: <ul style="list-style-type: none"> 6. Information content is defined in terms of identified communication requirements; 7. Parties to communicate with are identified 8. The party responsible for the communication is identified. 9. Events that require communication actions are identified. 10. The channel for the communication is selected. 11. Information products are communicated to relevant interested parties.
Base Practices	<p>COM.01.BP1 Define information content. Define information content in terms of identified communication needs and requirements. [Outcome 1]</p> <p>COM.01.BP2 Identify parties to communicate to. Identify parties to communicate with. [Outcome 2]</p> <p>COM.01.BP3 Identify party responsible for communication. Identify the party responsible for the communication. [Outcome 3]</p> <p>COM.01.BP4 Identify communication events. Identify the events that require communication actions.[Outcome 4]</p> <p>COM.01.BP5 Select communication channel. Select the channel for the communication. [Outcome 5]</p>

	COM.01.BP6 Communicate information products. Communicate information products to relevant interested parties. [Outcome 6]
--	--

9.3.2.2 COM.02 Documentation management

Process ID	COM.02
Process Name	Documentation management <i>[ref]</i>
Comment	<p>Ref: ISO/IEC 33073 COM.02</p> <p>Base Practices of COM.02: first outcomes from ISO/IEC 33073 has been put as last outcome. Second outcome from ISO/IEC 33073 has become first outcome, and “Documented information” at the beginning of sentence has been replaced by “Information”.</p> <p>Note 1: “Quality management system” has been replaced by “risk management framework”</p> <p>Note 2: This process covers “Recording and reporting” from ISO 31000.</p>
Process Purpose	The purpose of Documentation management is to provide relevant, timely, complete, valid documented information to designated parties.
Process Outcomes	<p>As a result of successful implementation of the Documentation management process:</p> <ol style="list-style-type: none"> 1. Information to be documented is identified. 2. The forms of documented information representation are defined. 3. The documented information content status is known. 4. Documented information is current, complete and valid. 5. Documented information is released according to defined criteria. 6. Documented information is available to relevant interested parties. 7. Documented information is archived, or disposed of, as required.
Base Practices	<p>COM.02.BP1 Information to be documented and managed is identified. Identify information of internal and external origin to be documented and necessary for the operation of the risk management framework. [Outcome 1]</p> <p>COM.02.BP2 The forms of documented information representation are defined. Identify the forms of information to be stored in the repository. For example, this may include documents, records, audio content, video content, image content. [Outcome 2]</p>

	<p>COM.02.BP3 The documented information content status is known. The status of the documented information content refers to the timeliness of the information content. This includes the control of changes, for example, by using version control techniques. [Outcome 3]</p> <p>COM.02.BP4 Documented information is current, complete and valid. The documented information contained in the repository is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity). [Outcome 4]</p> <p>COM.02.BP5 Documented information is released according to defined criteria. The documented information release status refers to those situations typically where authorisation is needed, such as in situations where: a) agreements are in force, b) policies and procedures are approved by management and their use in the organization is thereby obligatory. [Outcome 5]</p> <p>COM.02.BP6 Documented information is available to relevant interested parties. Manage the distribution, access, retrieval and use of documented information towards interested parties. [Outcome 6]</p> <p>COM.02.BP7 Documented information is archived, or disposed of, as required. Manage documented information, including records, through its lifecycle by addressing the following activities:</p> <ul style="list-style-type: none"> - storage and preservation, including preservation of legibility - retention and disposition. <p>Note: Records should be protected in accordance with statutory, regulatory, contractual and business requirements. [Outcome 7]</p>
--	--

9.3.2.3 COM.03 Human resource management

Process ID	COM.03
Process Name	Human resource management <i>[ref]</i>
Comment	Ref ISO/IEC 33073 COM.03 Required resources for performing risk management activities are identified in COM.08 Operational planning process.
Process Purpose	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.

Process Outcomes	As a result of successful implementation of the Resource management process: <ol style="list-style-type: none"> 1. The competencies required by the organization to produce products and services are identified. 2. Identified competency gaps are filled through training or recruitment. 3. Understanding of roles and activities in achieving organisational objectives in product and service provision is demonstrated by each individual.
Base Practices	<p>COM.03.BP.1 Identify organizational competencies. Identify the competencies required by the organization. [Outcome 1]</p> <p>COM.03.BP.2 Fill competency gaps. Fill identified competency gaps through training or recruitment. [Outcome 2]</p> <p>COM.03.BP.3 Demonstrate awareness of understanding of role. Each individual demonstrates their understanding of their role and activities in achieving organizational objectives. [Outcome 3]</p>

9.3.2.4 COM.04 Improvement

Process ID	COM.04
Process Name	Improvement
Comment	Ref ISO/IEC 33073 COM.04 Quality management system” has been replaced by “Risk management framework”. “Management reviews” has been replaced by “Monitoring and review”.
Process Purpose	The purpose of Improvement is to continually improve the risk management framework and its processes.
Process Outcomes	As a result of successful implementation of the Improvement process: <ol style="list-style-type: none"> 1. Opportunities for improvement are identified. 2. Opportunities for improvement are evaluated against defined criteria 3. Improvements are prioritised. 4. Improvements are implemented. 5. The effectiveness of implemented improvements is evaluated.
Base Practices	<p>COM.04.BP.1 Identify improvement opportunities. These might arise from the following sources:</p> <p>a) The decisions and actions arising from the outputs of the monitoring and reviews;</p>

	<p>b) feedback arising from actions to meet customer requirements and assess customer satisfaction;</p> <p>c) actions arising from i) improving products and services to meet requirements as well as to address future needs and expectations; ii) correcting, preventing or reducing undesired effects; iii) improving the performance and effectiveness of the risk management framework. [Outcome 1]</p> <p>COM.04.BP.2 Evaluate improvement opportunities. Evaluate opportunities for improvement against defined criteria. The results of analysis are used to evaluate the need for improvements to the risk management framework, and to the business processes. [Outcome 2]</p> <p>COM.04.BP.3 Prioritise improvements. Prioritise the improvements to be made. [Outcome 3]</p> <p>COM.04.BP.4 Implement improvements. Implement the selected improvements. [Outcome 4]</p> <p>COM.04.BP.5 Evaluate improvement effectiveness. Evaluate the effectiveness of implemented improvements. [Outcome 5]</p>
--	---

9.3.2.5 COM.05 Internal audit

Process ID	COM.05
Process Name	Internal audit <i>[ref]</i>
Comment	Ref ISO/IEC 33073 COM.05
Process Purpose	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.
Process Outcomes	<p>As a result of successful implementation of the Internal audit process:</p> <ol style="list-style-type: none"> 1. The scope and purpose of each audit is defined. 2. The objectivity and impartiality of the conduct of audits and selection of auditors are assured. 3. Conformity of selected services, products and processes with requirements, plans and agreements is determined.

Base Practices	COM.05.BP1 Define the criteria and scope of each audit. Define the audit criteria and the scope of each audit. [Outcome 1]
	COM.05.BP2 Select auditors. Select auditors to ensure objectivity and the impartiality of the audit process. [Outcome 2]
	COM.05.BP3 Conduct audits. Conduct audits according to the defined criteria ensuring objectivity and the impartiality of the audit process. [Outcome 3]

9.3.2.6 COM.06 Monitoring and review

Process ID	COM.06
Process Name	Monitoring and review
Comment	Ref ISO/IEC 33073 COM.06 Management review Note: “Management review” has been replaced by “Monitoring and review”. The purpose of monitoring and review in ISO 31000 is: to assure and improve the quality and effectiveness of process design, implementation and outcomes.
Process Purpose	The purpose of Monitoring and review is to assess the performance of the risk management framework, to identify and make decisions regarding potential improvements.
Process Outcomes	As a result of successful implementation of the Monitoring and review process: <ol style="list-style-type: none"> 1. The objectives of the monitoring and review are established. 2. The status and performance of an activity or process are assessed in terms of the established objectives. 3. Risks, problems and opportunities for improvement are identified.
Base Practices	COM.06.BP1 Identify the objectives for monitoring and review. Objectives for monitoring and reviewing the risk management framework include: <ul style="list-style-type: none"> - the status of actions from previous reviews into consideration - consideration of changes in external and internal issues that are relevant to the risk management framework - consider the information on the risk management performance - consider the feedback from interested parties. - consider the results of risk assessment and status of risk treatment plan - consider the opportunities for continual improvement. [Outcome 1]

	<p>COM.06.BP2 Assess status and performance of activities. Management conduct monitoring and reviews of the organization’s risk management framework to ensure its continuing suitability, adequacy and effectiveness. [Outcome 2]</p> <p>COM.06.BP3 Identify risks, problems and opportunities for improvement. Identify risks, problems, and opportunities related to improvement, and the need for changes to the risk management framework. [Outcome 3]</p>
--	---

9.3.2.7 COM.07 Non-conformity management

Process ID	COM.07
Process Name	Non-conformity management
Process Context	Ref: ISO/IEC 33073 COM.07 Note: “Quality management system” has been replaced by “risk management framework”
Process Purpose	The purpose of Non-conformity management is to resolve non-conformities and to eliminate their causes when appropriate.
Process Outcomes	<p>As a result of successful implementation of the Non-conformity management process:</p> <ol style="list-style-type: none"> 1. Non-conformities are identified. 2. Non-conformities are resolved and closed. 3. The cause(s) of selected non-conformities is determined. 4. The need for action to eliminate the causes of non-conformities is evaluated. 5. A selected action proposal is implemented. 6. The effectiveness of changes to eliminate the non-conformities is confirmed
Base Practices	<p>COM.07.BP1 Identify non-conformities. Non-conformities are identified. These might arise during development and/or production of the product/service, or from post-production activities e.g. feedback from customers. [Outcome 1]</p> <p>COM.07.BP2 Resolve and close non-conformities. Resolve and close non-conformities. When a nonconformity occurs, including any arising from complaints, the organization</p>

	<p>a) reacts to the nonconformity and, as applicable:</p> <ul style="list-style-type: none"> i) take action to control and correct it; ii) deal with the consequences. [Outcome 2] <p>COM.07.BP3 Determine cause of non-conformities. Determine the cause of selected non-conformities.</p> <p>The organization evaluates the need for action to eliminate the cause(s) of the non-conformity, in order that it does not recur or occur elsewhere, by:</p> <ul style="list-style-type: none"> i) reviewing and analysing the non-conformity; ii) determining the causes of the non-conformity; iii) determining if similar non-conformities exist, or could potentially occur. [Outcome 3] iv) <p>COM.07.BP4 Determine the need for action. Determine the need for action to eliminate the causes of non-conformities. Corrective actions are appropriate to the effects of the nonconformities encountered. [Outcome 4]</p> <p>COM.07.BP5 Implement selected action proposals. Implement a selected action proposal. The organisation implements any action needed. If necessary, changes are made to the risk management framework. [Outcome 5]</p> <p>COM.07.BP6 Confirm change effectiveness. Confirm the effectiveness of changes to eliminate the non-conformities. The organization reviews the effectiveness of any corrective action taken. [Outcome 6]</p>
--	--

9.3.2.8 COM.08 Operational planning

Process ID	COM.08
Process Name	Operational planning
Comment	Ref ISO/IEC 33072 COM.08
Process Purpose	The purpose of Operational Planning is to define the characteristics of all operational and organizational processes, and to plan their execution.
Process Outcomes	As a result of successful implementation of this process: <ul style="list-style-type: none"> 1. Process requirements are identified. 2. Process input and output products are determined. 3. The set of activities that transform the inputs into outputs is determined.

	<p>4. The sequence and interaction of the process with other processes is determined.</p> <p>5. The required competencies and roles for performing the process are identified.</p> <p>6. The required resources for performing the process are identified.</p> <p>7. Methods for monitoring the effectiveness and suitability of the process are determined.</p> <p>8. Plans for the deployment of the process are developed.</p>
<p>Base Practices</p>	<p>COM.08.BP1 Identify process needs and requirements. Identify process needs and requirements. [Outcome 1]</p> <p>COM.08.BP2 Determine process input and output products. Determine process input and output products. [Outcome 2]</p> <p>COM.08.BP3 Identify documented information to be managed. Identify documented information of internal and external origin necessary for the operation of the risk management framework. [Outcome 3]</p> <p>COM.08.BP3 Identify process needs and requirements. Identify process needs and requirements. [Outcome 3]</p> <p>COM.08.BP3 Determine the set of activities that transform the inputs into outputs. Determine the set of activities that transform the inputs into outputs. [Outcome 3]</p> <p>COM.08.BP4 Determine the sequence and interaction of the process with other processes. Determine the sequence and interaction of the process with other processes. [Outcome 4]</p> <p>COM.08.BP5 Identify the required competencies and roles for performing the process. Identify the required competencies and roles for performing the process. [Outcome 5]</p> <p>COM.08.BP6 Identify the required resources for performing the process. Determine what resources will be required by the risk management framework to achieve its risk objectives. Make projections of future capacity requirements to ensure the required system performance. [Outcome 6]</p> <p>COM.08.BP7 Determine the methods for monitoring the effectiveness and suitability of the process. Determine the methods for monitoring the effectiveness and suitability of the process. [Outcome 7]</p>

	COM.08.BP8 Plan the deployment of the process. Plan the processes will be deployed in order to achieve the risk objectives. [Outcome 8]
--	--

9.3.2.9 COM.09 Operational implementation and control

Process ID	COM.09
Process Name	Operational implementation and control
Comments	Source ISO/IEC 33072 COM.09
Process Purpose	The purpose of Operational implementation and control is to deploy and control the execution and performance of operational and organisational processes.
Process Outcomes	<p>As a result of successful implementation of this process:</p> <ol style="list-style-type: none"> 1. The required roles, responsibilities and authorities are allocated. 2. The required resources are allocated and applied. 3. Actions required to achieve the management framework objectives are implemented. 4. Suitability and effectiveness of the actions taken to achieve the management framework objectives are reviewed. 5. Deviations from planned arrangements are corrected when targets are not achieved. 6. Data is collected and analysed as a basis for understanding the behaviour of, and to demonstrate the suitability and effectiveness of the processes.
Base Practices	<p>COM.09.BP1 Allocate roles, responsibilities and authorities. Allocate the required roles, responsibilities and authorities. [Outcome 1]</p> <p>COM.09.BP2 Allocate resources. Allocate and apply the required resources. [Outcome 2]</p> <p>COM.09.BP3 Perform process activities. Implement actions taken to achieve the risk management framework objectives. [Outcome 3]</p> <p>COM.09.BP4 Review process activities. Review suitability and effectiveness of the actions required to achieve the management framework objectives. [Outcome 4]</p>

	<p>COM.09.BP5 Correct deviations. Correct deviations from planned arrangements when targets are not achieved. [Outcome 5]</p> <p>COM.09.BP6 Collect and analyse data. Collect and analyse data as a basis for understanding the behaviour of, and to demonstrate the suitability and effectiveness of the processes. [Outcome 6]</p>
--	--

9.3.2.10 COM.10 Performance evaluation

Process ID	COM.10
Process Name	Performance evaluation
Comments	<p>Ref ISO/IEC 33073 COM.10</p> <p>“Quality management system” replaced by “Risk management framework”</p>
Process Purpose	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.
Process Outcomes	<p>As a result of successful implementation of this process:</p> <ol style="list-style-type: none"> 1. Performance monitoring and measurement needs are defined. 2. Performance measures, derived from the performance measurement needs, are identified. 3. Performance measurement methods, supportive of the performance measures, are identified. 4. Data is collected using the identified performance measurement methods. 5. The collected performance data is analyzed.
Base Practices	<p>COM.10.BP.1 Determine what needs to be monitored. Determine what needs to be monitored and measured. [Outcome 1]</p> <p>COM.10.BP.2 Determine appropriate performance measures. Determine appropriate performance measures that support the performance measurement needs. [Outcome 2]</p> <p>COM.10.BP.3 Determine the appropriate methods for monitoring, measurement, analysis and evaluation. Determine the appropriate methods for monitoring, measurement, analysis and evaluation as well as how the results will be evaluated. [Outcome 3]</p>

COM.10.BP.4 **Monitor and measure the risk management framework performance.**

Collect and verify data on the risk management framework performance of the organization. [Outcome 4]

COM.10.BP.5 **Analyse the collected data.** Analyze the collected data in order to evaluate the risk management framework performance, the effectiveness of the risk management framework as well as the effectiveness of any action taken within the scope of the risk management framework. [Outcome 5]

9.3.3 Risk Management Processes

9.3.3.1 RIS.01 Risk criteria definition

Process ID	RIS.01
Process Name	Risk criteria definition
Comment	Specific risk management process
Process Purpose	The purpose of Risk criteria definition is to set and continually update risk criteria according to scope, context and objectives of the organization.
Process Outcomes	As a result of successful implementation of the Risk criteria definition process: <ul style="list-style-type: none"> 1. Organizational specifications for risk criteria are identified. 2. Risk criteria are set by defining the aspects that characterize a risk 3. Risk criteria are continually reviewed and amended if necessary.
Base Practices	<p>RIS.01.BP1. Identify organizational specifications for risk criteria. [Outcome 1]</p> <p>RIS.01.BP2. Set risk criteria by defining the way risks are assessed. [Outcome 2]</p> <p>Note: examples of "aspects/things" to be considered to set the risk criteria, can be consequences, likelihood, time-related factors...</p> <p>RIS.01.BP3. Continually review risk criteria and amend if necessary. [Outcome 3]</p>
ISO/IEC 27001 view for BP2	<p>The organization shall define and apply an information security risk assessment process that:</p> <p>a) establishes and maintains information security risk criteria that include:</p> <ul style="list-style-type: none"> 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;

Input Work Product
ID & Name

Output Work Product
ID & Name
Risk criteria

9.3.3.2 RIS.02 Risk identification

Process ID	RIS.02
Process Name	Risk identification
Comment	Specific risk management process
Process Purpose	The purpose of Risk identification is to find and describe risks that might help or prevent an organization from achieving its objectives.
Process Outcomes	As a result of successful implementation of the Risk identification process: <ul style="list-style-type: none"> 1. Relevant information and risk identification techniques are selected 2. Factors of risks and their relationships are examined. 3. Risks are identified, based on factors of risks.
Base Practices	RIS.02.BP1. Gather relevant and up-to-date information for the identification of risks (appropriate background information where possible) [Outcome 1] RIS.02.BP2. Select context relevant risk identification tools and techniques. [Outcome 1]

	<p>RIS.02.BP3. Examine a set of factors for identifying risks (Tangible and intangible sources of risk, Causes and events, Threats and opportunities, Vulnerabilities and capabilities ,...) [Outcome 2]</p> <p>RIS.02.BP4. Identify risks based on factors of risks. [Outcome 3]</p>
ISO 21500 view	<p>For BP1: information comes as the project progresses through its life cycle</p> <p>For BP4: Identification of risks with a potential negative impact (threats); Identification of risks with a potential positive impact (opportunities)</p> <p>Input Work Products: Project plans</p> <p>Output Work Products: Risk register</p>
ISO/IEC 27001 & ISO/IEC 27005 views	<p>For BP1: Information comes from the information security risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system</p> <p>For BP4: Identification of assets; Identification of threats; Identification of existing controls; Identification of existing vulnerabilities; Identification of consequences</p> <p>Input Work Products: Scope and boundaries for the risk assessment, list of constituents with owners, location, function, etc.</p> <p>Output Work Products: A list of incident scenarios with their consequences related to assets and business processes identification</p>

Input Work Product
ID & Name
Risk management plan

Output Work Product	
ID & Name	
Risk register (list of risks)	

9.3.3.3 RIS.03 Risk analysis

Process ID	RIS.03
Process Name	Risk analysis
Comment	Specific risk management process
Process Purpose	The purpose of Risk analysis is to determine a level of risk from analysis techniques and factors of risks.
Process Outcomes	<p>As a result of successful implementation of the risk analysis process:</p> <ol style="list-style-type: none"> 1. Appropriate analysis techniques are selected. 2. Factors of risks are considered including influences. 3. A level of risk is determined. 4. Risk analysis results are recorded. 5. Risk analysis results are communicated to decision makers.
Base Practices	<p>RIS.03.BP1. Select analysis techniques that are appropriate depending on circumstances and intended use. [Outcome 1]</p> <p>RIS.03.BP2. Identify the factors of risks to consider. These factors can be: likelihood of events and consequences, the nature and magnitude of consequences, complexity and connectivity, time-related factors and volatility, pace of change, effectiveness of existing controls, sensitivity and confidence levels, influences (any divergence of opinions, biases, perceptions of risk and judgements; additional influences: the quality of the information used, the assumptions and exclusions made, any limitations of the techniques and how they are executed). [Outcome 2]</p>

	<p>RIS.03.BP3. Determine a level of risks considering uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. [Outcome 3]</p> <p>RIS.04.BP4. Record risk analysis results. [Outcome 4]</p> <p>RIS.03.BP5. Communicate risk analysis results to decision makers. [Outcome 5]</p>
ISO 21500 view	<p>For BP3: Estimate the probability of occurrence of each risk; Estimate the corresponding consequence for project objectives.</p> <p>Input Work Products: Risk register; Project plans</p> <p>Output Work Products: Measured risks</p>
ISO/IEC 27001 & ISO/IEC 27005 views	<p>For BP1: 8.3.1 Risk analysis methodologies (qualitative, quantitative)</p> <p>For BP3: 8.3.2 Assessment of consequences (assets identification, assessment of business impact in terms of Confidentiality, Integrity, Availability); 8.3.3 Assessment of incident likelihood (likelihood of incident scenarios : quanti or quali); 8.3.4 Level of risk determination; Issue a list of risks with value levels assigned</p> <p>Input Work Products: List of identified relevant incident scenarios</p> <p>Output Work Products: List of risks with value levels assigned</p>

Input Work Product
ID & Name
Risk register (list of risks)

Output Work Product
ID & Name
Risks analysis results (level of risks)

9.3.3.4 RIS.04 Risk evaluation

Process ID	RIS.04
Process Name	Risk evaluation
Comment	Specific risk management process
Process Purpose	The purpose of Risk evaluation is to support decisions.
Process Outcomes	As a result of successful implementation of the Risk evaluation process: <ol style="list-style-type: none"> 1. The significance of risks is determined by comparing analysed risks to risk criteria. 2. A decision is made based on the determined significance of risks. 3. Evaluated risks are recorded. 4. Evaluated risks are communicated at appropriate levels of the organisation. 5. Evaluated risks are validated at appropriate levels of the organisation.
Base Practices	<p>RIS.04.BP1. Compare analysed risks to risk criteria.</p> <p>RIS.04.BP2. Decide what to do for each risk according to its significance.</p> <p>RIS.04.BP3. Record the evaluated risks issued from the comparison of analysed risks to risk criteria.</p> <p>RIS.04.BP4. Communicate the evaluated risks to stakeholders.</p> <p>RIS.04.BP5. Validate the evaluated risks at appropriate levels of the organisation.</p>
ISO 21500 view	<p>For BP2: Risks are prioritized considering factors such as timeframe and key stakeholders' risk tolerance.</p> <p>Input Work Products: Measured risks (probability and consequences)</p> <p>Output Work Products: Prioritized risks</p>
ISO/IEC 27001 & ISO/IEC 27005 views	<p>For BP2: Decisions are mainly based on the acceptable level of risk</p> <p>Input Work Products: List of risks with value levels assigned; Risk evaluation criteria</p> <p>Output Work Products: List of prioritized risks</p>

Input Work Product
ID & Name
Analysed risks
Risk criteria

Output Work Product
ID & Name
Evaluated risks record

9.3.3.5 RIS.05 Risk treatment

Process ID	RIS.05
Process Name	Risk treatment
Process Purpose	The purpose of Risk treatment is to select and implement options for addressing risk.
Comment	Specific risk management process
Process Outcomes	<p>As a result of successful implementation of the Risk treatment process:</p> <ol style="list-style-type: none"> 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.

<p>Base Practices</p>	<p>RIS.05.BP1. Select risk treatment options. For selecting risk treatment options, consider the organization's objectives, risk criteria and available resources. [Outcome 1]</p> <p>RIS.05.BP2. Specify selected risk treatment options with appropriate information for justification, implementation, integration and documentation in a risk treatment plans. [Outcome 2]</p> <p>RIS.05.BP3. Execute risk treatment plans for remaining risks and new risks. [Outcome 3]</p> <p>RIS.05.BP4. Communicate remaining risks to decision makers and other stakeholders. [Outcome 4]</p> <p>RIS.05.BP5. Update risk changes in the risk register. [Outcome 5]</p>
<p>ISO 21500 view</p>	<p>For BP1: Insertion of resources and activities into the budget and schedule</p> <p>For BP2: 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.</p> <p>Input Work Products: Risk register ; Project plans</p> <p>Output Work Products: Risk responses; Change requests; Risk register</p>
<p>ISO/IEC 27001 & ISO/IEC 27005 views</p>	<p>For BP1: Selection of appropriate information security treatment options, taking into account of the risk assessment results</p> <p>For BP2: Formulate an information security risk treatment plan.</p> <p>FOR BP3: Determine all controls that are necessary to implement the information security risk treatment options chosen.</p> <p>For BP4: Obtain risk owner's approval of the information security risk treatment plan and acceptance of the residual information security risks.</p> <p>For BP5: The organization shall retain documented information about the information security risk treatment process.</p> <p>Input Work Products: Information security risk treatment plan</p>

Input Work Product

ID & Name
Risk register Risk criteria

Output Work Product
ID & Name
Risk treatment plans Remaining risks Risk register

9.4 Process capability indicators for level 1 to 5

The process capability indicators related to the process attributes associated with capability levels 1 to 5 are defined in ISO/IEC 33020. Process capability indicators are the means of achieving the capabilities addressed by the considered process attributes. Evidence of process capability indicators supports the judgment of the degree of achievement of the process attribute.

10. References

1. Barafort, B., Di Renzo B., Merlan O., Benefits resulting from the combined use of ISO/IEC 15504 with the Information Technology Infrastructure Library (ITIL), in: *Proceedings of the International Conference PROFES'2002*, Rovaniemi, Finland, 2002
2. ISO/IEC 15504 Information technology — Process assessment, Parts 1-10 (2003, 2012)
3. The Cabinet Office. IT Infrastructure Library - Service Strategy; Service Design; Service Transition; Service Operation; Continuous Service Improvement. The Stationery Office Edition (2011)
4. Barafort, B., Rousseau, A., Sustainable Service Innovation Model: a standardized IT Service Management Process Assessment framework, in: *Proceedings of the International Conference EuroSPI 2009*, Madrid, Spain, 2009
5. ISO/IEC 20000-1 Information technology — Service management — Part 1: Service management system requirements (2011)
6. 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, in: *Proceedings of the International Conference SPICE 2008*, Nuremberg, Germany, 2008
7. Mangin, O., Barafort, B., Dubois, E., Heymans, P., Designing a Process Reference Model for Information Security Management Systems, in: *Proceedings of the International Conference SPICE 2012*, Mallorca, Spain, 2012
8. Mangin, O., Mayer, N., Barafort, B., Dubois, E., Heymans, P., An improvement of process reference model design and validation using business process management, in: *Proceedings of the International Conference SPICE 2013*, Bremen, Germany, 2013
9. Cortina, S., Mayer, N., Renault, A., Barafort, B., Towards a Process Assessment Model for Management System Standards, to be published in: *Proceedings of the International Conference SPICE 2014*, Vilnius, Lithuania, 2014
10. Cortina, S., Renault, A., Barafort, B., Towards a Maturity Model for ISO/IEC 20000-1 based on the TIPA for ITIL Process Capability Assessment Model, 15th International SPICE Conference on Process Improvement and Capability dEtermination in Software, Systems Engineering and Service Management (SPICE2015), Gothenburg, Sweden, June 2015.
11. Picard, M., Renault, A., Barafort, B., A Maturity Model for ISO/IEC 20000-1 based on the TIPA for ITIL Process Capability Assessment Model, 22nd European & Asian System, Software & Service Process Improvement & Innovation (EuroAsiaSPI'15), Ankara, Turkey, October 2015.
12. Mesquida, A., Mas Pichaco, A., Barafort, B., The Project Management SPICE (PMSPICE) Process Reference Model: Towards a Process Assessment Model, in 22nd European & Asian System, Software & Service Process Improvement & Innovation (EuroAsiaSPI'15), Ankara, Turkey, October 2015.
13. Barafort, B., Betry V., Cortina, S., Picard, M., St-Jean, M., Renault, A., Valdés, O., ITSM Process Assessment supporting ITIL® - Using TIPA to Assess and Improve your Processes with ISO 15504 and Prepare for ISO 20000 Certification, Van Haren Publishing, ISBN 9789087535643, The Netherlands, 2009, ISBN: 9789087535643.
14. Renault, A., Barafort, B., TIPA: 7 years experience with SPICE for IT Service Management in: *Proceedings of the International Conference EuroSPI 2011*, Roskilde, Denmark, 2011
15. Renault, A., Barafort, B., TIPA for ITIL from Genesis to Maturity of SPICE Applied to ITIL 2011 in: *Industrial Proceedings of the 21st International Conference EuroSPI² 2014*, Luxembourg, 2014
16. Barafort, B., Rousseau, A., Dubois, E., How to Design an Innovative Framework for Process Improvement? The TIPA for ITIL Case in: *Proceedings of the International Conference EuroSPI 2014*, Luxembourg, 2014
17. ISO/IEC JTC1 SC7. <https://www.iso.org/committee/45086.html> (online: accessed 08-July-2018) (2016)
18. ISO/IEC JTC1 SC40. <https://www.iso.org/committee/5013818.html> (online: accessed 08-July-2018) (2016)
19. ISO Guide 73, Risk management — Vocabulary. International Organization for Standardization, Geneva (2009)
20. ISO/IEC Directives, Part1. Annex SL Proposals for management system standards. International Organization for Standardization, Geneva (2018)
21. ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization, Geneva (2013)
22. ISO 9001: Quality management systems – Requirements. International Organization for Standardization, Geneva (2015)
23. Automotive Spice, http://www.automotivespice.com/fileadmin/software-download/Automotive_SPICE_PAM_30.pdf (online: accessed 20-May-2018) (2016)
24. TIPA for ITIL, https://www.list.lu/fileadmin//files/projects/ TIPA_T10_ITIL_PAM_r2_v4.1.pdf (online: accessed 20-May-2018) (2015)
25. ISO/IEC 15504-8: Information Technology – Process assessment – An exemplar process assessment model for IT service management. International Organization for Standardization, Geneva (2012)
26. Lepmets, M., McCaffery, F., & Clarke, P. Development and benefits of MDevSPICE®, the medical device software process assessment framework. *Journal of Software: Evolution and Process*, 28(9), 800-816. (2016)
27. ISO/IEC 33001: Information Technology - Process assessment – Concepts and terminology. International Organization for Standardization, Geneva (2015)

28. Afnor normalisation, Standardization: a Genuine Advantage for the Economic Activity of Companies that get Involved in it, Association Française de Normalisation, Paris (2016)
29. <http://www.iso.org/iso/home/standards/benefitsofstandards.htm> (online: accessed 08-July-2018) (2017)
30. <http://www.iso.org/iso/home/standards/management-standards.htm> (online: accessed 08-July-2018) (2017)
31. ISO Survey 2017. <http://www.iso.org/iso/iso-survey> (online: accessed 19-September-2018) (2018)
32. 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
33. ISO 21500: Guidance on project management. International Organization for Standardization, Geneva (2012)
34. ISO 31000: Risk management – Principles and guidelines. International Organization for Standardization, Geneva (2018)
35. 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.
36. 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.
37. 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.
38. Larrucea, X., & Santamaria, I. (2014). An industrial assessment for a multimodel framework. *Journal of Software: Evolution and Process*, 26(9), 837-845.
39. 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*.
40. 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.
41. 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.
42. Pardo, C., Pino, F. J., García, 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.
43. 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.
44. Casadesús, M., Karapetrovic, S., Heras, I.: Synergies in standardized management systems: Some empirical evidence. *TQM J.* 23(1), 73–86 (2011). Emerald Insight
45. Simon, A., Karapetrovic, S., Casadesús, M.: Difficulties and benefits of integrated management systems. *Ind. Manage. Data Syst.* 112(5), 828–846 (2012). Emerald Insight
46. 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*, 4(4), 27-47 (2016)
47. ISO/IEC 27013: TS Information Technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1. International Organization for Standardization, Geneva (2015)
48. Mesquida, A.L., Mas, A.: Integrating IT service management requirements into the organizational management system. *Comput. Stand. Interfaces* 37, 80–91 (2015). Elsevier
49. 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
50. 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
51. ISO/IEC 20000-1 Information technology — Service management — Part 1: Service management system requirements (2018)
52. ISO/IEC 33072: TS Information Technology — Process Assessment — Process capability assessment model for information security management. International Organization for Standardization, Geneva (2016)
53. ISO/IEC 20000-4 Information technology — Service management — Part 4: Process reference model (2010)
54. ISO 31000: Risk management – Principles and guidelines. International Organization for Standardization, Geneva (2009)
55. ISO/IEC 27005: Information technology– Security techniques – Information security risk management – Requirements. International Organization for Standardization, Geneva (2018)
56. Parra, A. S. O., Crespo, L. E. S., Alvarez, E., Huerta, M., & Paton, E. F. M. Methodology for Dynamic Analysis and Risk Management on ISO27001. *IEEE Latin America Transactions*, 14(6), 2897-2911 (2016)
57. Chou, D. C. Cloud computing risk and audit issues. *Computer Standards & Interfaces*, 42, 137-142 (2015)
58. 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)

59. 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)
60. Chittister C. and Haimes. Y. Y. Risk associated with software development: a holistic framework for assessment and management, *IEEE Transactions on Systems, Man, and Cybernetics*, 23, 3, 710-723, May/June (1993)
61. Lyytinen, K., Mathiassen, L., Ropponen, J., A Framework for software risk management, *Journal of Information Technology*, 11, 4, 1996, 275-285 (1996)
62. Bandyopadhyay, K., Mykytyn, P.P., Mykytyn, K., A framework for integrated risk management in information technology", *Management Decision*, Vol. 37 Issue: 5, pp.437-445 (1999)
63. Kontio, J., Software Engineering Risk Management: A Method, Improvement Framework, and Empirical Evaluation. Doctoral dissertation (2001)
64. Roy, G.G. A risk management framework for software engineering practice, 2004 Australian Software Engineering Conference. Proceedings, 2004, pp. 60-67 (2004)
65. Risk Management Framework, SEI, Christopher J. Alberts and Audrey J. Dorofee. TECHNICAL REPORT. CMU/SEI-2010-TR-017. ESC-TR-2010-017 (2010)
66. Buglione, L., Abran, A., von Wangenheim, C. G., McCaffery, F., & Hauck, J. C. R., 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)
67. ISO/IEC 15504-5. Information Technology – Process assessment – An exemplar software life cycle process assessment model. International Organization for Standardization, Geneva (2012)
68. 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)
69. Javaid, M. I., & Iqbal, M. M. W. 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)
70. Varajão, J., Colomo-Palacios, R., & Silva, H. ISO 21500: 2012 and PMBoK 5 processes in information systems project management. *Computer Standards & Interfaces*, 50, 216-222 (2017)
71. Öbrand, L., Holmström, J., & Newman, M. Navigating Rumsfeld's quadrants: A performative perspective on IT risk management. *Technology in Society* (2017)
72. Pries-Heje, J., & Johansen, J. Spi manifesto. *European System & Software Process Improvement and Innovation* (2010)
73. ISO/IEC/IEEE CD 16085: Systems and software engineering -- Life cycle processes -- Risk management. International Organization for Standardization, Geneva (2018)
74. 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)
75. Becker, J., Knackstedt, R., & Pöppelbuß, J. Developing maturity models for IT management. *Business & Information Systems Engineering*, 1(3), 213-222 (2009)
76. 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)
77. ISO/IEC 33004: Information Technology – Process assessment – Requirements for process reference, process assessment and maturity models. International Organization for Standardization, Geneva (2015)
78. Gresse von Wangenheim, Hauck J.C.R., Zoucas A., Salviano C.F., McCaffery F., ShullF., Creating Software Process Capability/Maturity Models, *IEEE Software*, Vol.27, No.4, July-Aug 2010, pp.92-94 (2010)
79. Stallinger, Fritz, and Reinhold Plösch. 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)
80. Di Renzo, B., et al. "Operational risk management in financial institutions: Process assessment in concordance with Basel II." *Software Process: Improvement and Practice* 12.4: 321-330 (2007)
81. CMMI for Development, Acquisition & Services, version 1.3. Carnegie Mellon University, Software Engineering Institute (2010)
82. ISO/IEC 15504-2: Information Technology — Process assessment — Performing an assessment. International Organization for Standardization, Geneva (2003)
83. 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
84. 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
85. ISO/IEC 33073: TS Information Technology – Process Assessment – Process capability assessment model for quality management. International Organization for Standardization, Geneva (2017)

86. ISO 22301 Societal security - Business continuity management systems – Requirements. International Organization for Standardization, Geneva (2012)
87. ISO/IEC TR 90006 Guidelines for the application of ISO 9001:2008 to IT service management and its integration with ISO/IEC 20000-1:2011. International Organization for Standardization, Geneva (2013)
88. ISO/IEC 12207: Information technology – System and software engineering - Software lifecycle processes. International Organization for Standardization, Geneva (2008)
89. ISO/IEC/IEEE 15288: Information technology – System and software engineering - System lifecycle processes. International Organization for Standardization, Geneva (2015)
90. Enjeux – Le Magazine de la Normalisation et du Management. Association Française de Normalisation, Supplément N° 362, Paris (2016)
91. 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)
92. Guide A. Project Management Body of Knowledge (PMBOK® GUIDE). Project Management Institute (2001)
93. Buglione, L., Abran, A., von Wangenheim, C. G., McCaffery, F., & Hauck, J. C. R.: 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)
94. ISO, Economic benefits of standards – International case studies (ISBN 978-92-10556-7) (2014)
95. ISO/IEC 15504-6: Information Technology – Process assessment – An exemplar system life cycle process assessment model. International Organization for Standardization, Geneva (2013)
96. ISO/IEC 33071: TS Information Technology – Process Assessment – An integrated process capability assessment model for Enterprise processes. International Organization for Standardization, Geneva (2016)
97. ISO/IEC 30105-2: TS Information Technology – IT Enabled Services-Business Process Outsourcing (ITES-BPO) lifecycle processes – Process assessment model (PAM). International Organization for Standardization, Geneva (2016)
98. Automotive Spice, <https://goo.gl/BNu8c2> (online: accessed 22-January-2018) (2016)
99. Isaca: COBIT Process Assessment Model (PAM): Using COBIT 5 (ISBN:1604202718 9781604202717) (2013)
100. MacMahon, S. T., Cooper, T., & McCaffery, F. Revising IEC 80001-1: Risk Management of Health Information Technology Systems. Computer Standards & Interfaces (2018)
101. ISO 9000: Quality management systems – Fundamentals and vocabulary. International Organization for Standardization, Geneva (2015)
102. ISO/IEC 20000-10: TS Information Technology – Service management – Concepts and terminology. International Organization for Standardization, Geneva (2018)
103. ISO/IEC 27000: TS Information Technology – Security techniques – Information security management systems – Overview and vocabulary. International Organization for Standardization, Geneva (2016)
104. Denning, P. J., A New Social Contract for Research, in: Communications of the ACM (40:2) (1997), 132-134
105. March, S., and Smith, G. Design and natural science research on information technology, Decision Support Systems, 15, 4 (1995), 251–266.
106. Peffers, K., Tuunanen, T., Rothenberger, M., Chatterjee, S.: A design science research methodology for information systems research", Journal of Management Information Systems, 24(3) (2008)
107. ISO/IEC TR 24774: Software and systems engineering – Life cycle management – Guidelines for process description. International Organization for Standardization, Geneva (2010)
108. MacMahon, S. T., McCaffery, F., Eagles, S., Keenan, F., Lepmets, M., & Renault, A. Development of a process assessment model for assessing medical IT networks against IEC 80001-1. In *International Conference on Software Process Improvement and Capability Determination* (pp. 148-160). Springer, Berlin, Heidelberg (2012)
109. ISO/IEC 33020: Information Technology – Process assessment – Process measurement framework for assessment of process capability. International Organization for Standardization, Geneva (2015)
110. ISO, NP IWA 31 Using ISO 31000 guidance on risk management in management systems, <https://www.iso.org/standard/75812.html> (online: accessed 31-August-2018) (2018)
111. Renault, S., Cortina, S., & Valoggia. Designing a Process Assessment Model Based on Multiple Sources-A Procurement Case. In European Conference on Software Process Improvement (pp. 136-146). Springer, Cham (2018)
112. Scott, K. The unified process explained. Addison-Wesley Longman Publishing Co., Inc. (2002)