


# Mapping and Integrating Security and Risk Standards: a Systematic Literature Review

**André Fernandes**

(Universidade de Lisboa INOV-INESC INOVAÇÃO, Lisbon, Portugal

 <https://orcid.org/0000-0002-9709-0289>, [andre.d.fernandes@tecnico.ulisboa.pt](mailto:andre.d.fernandes@tecnico.ulisboa.pt))


**João Cruz**

(Universidade de Lisboa INOV-INESC INOVAÇÃO, Lisbon, Portugal

[joaopinhocruz@gmail.com](mailto:joaopinhocruz@gmail.com))


**Miguel Mira da Silva**

(Universidade de Lisboa INOV-INESC INOVAÇÃO, Lisbon, Portugal

 <https://orcid.org/0000-0002-0489-4465>, [mms@tecnico.ulisboa.pt](mailto:mms@tecnico.ulisboa.pt))

**Rúben Pereira**

(ISCTE - University Institute of Lisbon, Lisbon, Portugal

 <https://orcid.org/0000-0002-3001-5911>, [ruben.filipe.pereira@iscte-iul.pt](mailto:ruben.filipe.pereira@iscte-iul.pt))

**Abstract:** Organizations are under increasing pressure to comply with various rules, standards, and policies in today's regulatory environment. Compliance controls are put in place to avoid legal or regulatory violations, which could lead to severe penalties, loss of reputation, and financial damages. However, these controls may have similar scopes and objectives, resulting in duplicated work and unnecessary costs for the organizations. To address this issue, researchers carry out the mapping and integration of these standards to avoid duplication, streamline compliance efforts, and identify best practices. Our work aims to improve the State-of-the-Art by exploring the main benefits and problems resulting from these processes, as well as identifying methods or artifacts that can be reused in the future. We focus on the fields of Risk, Security, and Business Continuity, as these are critical areas where compliance is crucial for organizations. Through our research, we have found that current methods of generating mapping artifacts are not only cumbersome to execute but also ineffective, as they output a single artifact without the reasoning behind it.

**Keywords:** Mapping, Integration, Harmonization, Systematic Literature Review, Standards, Risk, Security, Business Continuity.

**Categories:** A, H

**DOI:** 10.3897/jucs.111677

## 1 Introduction

Organizations must manage their organizational risks to allow business continuity even in the face of adversity [Ritchie and Brindley, 2007]. To assist in ensuring business continuity, manage risks and improve business processes, some organizations have specialized in the creation and design of standardized frameworks. A standard method for organizations to improve their internal business processes is by implementing and getting certified in standards (such as ISO or NIST).

Organizations often opt to implement multiple of these compliance frameworks in their systems, with different goals for each. However, individually implementing each framework can prove to be a troublesome process [Simon et al., 2012]. The overlap of controls and processes between them can lead to confusion on the specifics of what is already implemented and what is not [Sheikhpour and Modiri, 2012]. Moreover, it can also be costly to adapt an organization's processes to meet the requirements of all standards separately [Yasin et al., 2020].

In addition to the issues mentioned above, the terms used to describe the same entity across different international standards are not always the same. Synonyms are common, especially between standards originating from different organizations or dealing with the same scopes in different contexts. Examples of this phenomenon include the standards ISO 27001 and COBIT [ISO/IEC 27001:2013, 2000, IT Governance Institute, 2007], which, despite their similarities in some controls, have fundamentally different focuses, especially in the sense that COBIT gives a more extensive governance-focused view when compared to ISO 27001 [Sheikhpour and Modiri, 2012].

This paper focuses on identifying which benefits and problems can arise from the mapping and integration of ISO/IEC standards and aggregate what methods or techniques exist within the literature to carry out these processes. In addition, we exclude any methods which involve software automation to carry out mappings or integrations of ISO/IEC standards.

In an effort to identify and address these questions, we conducted a Systematic Literature Review (SLR) [Kitchenham, 2004] which helped us identify the fundamental problems within this area of research: the high amount of time spent in the process of analyzing the gaps between different standards and their mappings [Mas et al., 2010]. Moreover, there are no readily available tools to assist in this process.

This paper follows the following structure: the sections Research Background and Related Work present the definitions for the most relevant concepts as well as a summary of similar papers on the topic. The Literature Review section is composed by three subsections, one for each stage of the SLR (Planning, Conducting, Reporting). In the Discussion section, we analyze the SLR findings in further detail. Finally, we conclude our paper, listing our work's limitations and identifying possible directions for future work.

## **2 Research Background and Related Work**

### **2.1 Research Background**

In this Subsection, we present the theoretical background for this paper and the main concepts that serve as the foundation for this paper, that can be found within Table 2. In order to achieve this goal, we base some of the definitions on those summarized in [Pardo et al., 2012].

### **2.2 Related Work**

In this subsection, we discuss related work in this field, why we believe the SLR conducted as part of this paper is relevant and what are its contributions.

Our main goal with this paper is to analyze the state of the art over the harmonization, mapping and integration of ISO/IEC standards. Before conducting an SLR on the topic, we searched for pre-existing secondary studies on the topic and found two papers.

Term	Definition
Harmonization	Activity that seeks to define and to configure the most suitable harmonization strategy for achieving the strategic goals of an organization where two or more models are involved.
Harmonization Strategy	A harmonization strategy is a process which is comprised of a set of methods and techniques defined systematically, which allows us to know “what to do”, as well as “how to put” two or more models in consonance with each other. In practice the Harmonization Strategy defines how to align the structures and terminologies of diverging models.
Mapping	Comparison technique applied to find the differences between the structures and semantics of the selected models.
Homogenization	Set of steps and tools by which one or more models are treated, to convert the structures of their process elements into homogeneous structures.
Ontology	An Ontology defines what exists for a given field or discipline. It is generally a levelled construct, with categories and subcategories grouping the lower-level elements. Ontologies are often used to map between models of the same field, providing keywords and a knowledge basis.
Control	Controls include, but are not limited to, any process, policy, practice, or other conditions and/or actions which maintain and/or modify the process or policy to be implemented.
Atomic Control	Indivisible control.
Metamodel	A model that consists of statements about models.
Process Reference Model (PRM)	A process reference model helps to define a set of processes which support objectives of a domain, and has two components: domain and scope, and purpose and process outcomes.
Coverage	Percentage of the atomic controls covered for a given construct.

*Table 1: Definitions of the most relevant terms*

In 2020, a group of researchers carried out a Multivocal Literature Review, in which the authors present their findings over the mapping of security standards across five sources (two of which were non-scientific) [Mussmann et al., 2020]. The article concludes that, despite the existence of some mappings, the current mapping methodologies are limited and should be further researched. Besides being older than our review, the mapping study [Mussmann et al., 2020] also differs from ours in three ways:

- We considered the Scopus database, a reliable source [Kitchenham, 2004] that is not included in the study carried out by Mussman et al. [Mussmann et al., 2020].
- We considered not only mappings, but also the integrations of standards.
- We considered all ISO/IEC standards related to risk, business continuity and security, not just security.

In addition to studies on mappings of standards [Mussmann et al., 2020], we have also identified secondary studies on integrations, but only over two integrations [Gunawan et al., 2020]. The authors concluded that integrating ISO/IEC 27001 [ISO/IEC 27001:2013, 2000] with COBIT [IT Governance Institute, 2007] and ITIL [Sandadi, 2017] brings similar benefits. Both integrations increase the credibility of information security, but while COBIT raises credibility on the governance side, ITIL does so on the IT management’s side.

We conclude that the studies share similar goals as compared to ours [Gunawan et al., 2020], however using different approaches. While their paper brought forward detailed information over two specific integrations, ours focuses on improving the state of the art across all the techniques used in the industry and academia to map and integrate ISO or IEC standards related to risk, business continuity and security.

### 3 Literature Review

An SLR is a research methodology that aims to produce a fair evaluation of a research topic through trustworthy, rigorous, and auditable means [Kitchenham, 2004, Keele et al., 2007]. Due to the credibility and trust that SLR artifacts elicit from their rigorous processes, we have opted to base this paper on this methodology and, as such, we carried out a three-stage process composed of the steps proposed by Kitchenham. A summary of these steps is given in Figure 1 [Kitchenham, 2004].

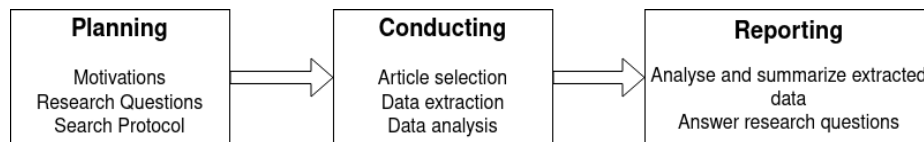


Figure 1: Summary of the methodology used

#### 3.1 Planning

In the Planning stage of this SLR, we described our methodology, including our motivations for the paper, the Research Questions (R.Q.) that we aimed to answer and the search protocol we drafted to collect and review the relevant articles.

##### 3.1.1 Motivation

To improve internal processes or even assist in reaching compliance with existing regulation [Lopes et al., 2019], the route organizations often pick is to seek certification in some international standards such as ISO/IEC. However, studies show that implementing multiple of these unintegrated standards can lead to reduced gains in performance with each additional implementation [Castillo-Rojas et al., 2012].

At the same time, some research has focused on analyzing the gaps between standards so as to reduce the amount of work needed to implement them [Gunawan et al., 2020, Musmann et al., 2020]. However, these research always focuses on either mappings or integrations, but never both. As such, we decided to review the state of the art on both of these processes with a single SLR.

##### 3.1.2 Research Questions

In this Sub-subsection, we present the Research Questions we aimed to answer during our literature review, with the first three questions focusing on the metadetails of mappings and integrations, and the latter two focusing on the artifacts generated from their respective processes.

We intended to discover whether the literature presented the mapping and integration of standards as a useful process, both in the industry and academia. To achieve this goal, we drafted R.Q. 1, in which we aimed to identify the benefits derived from the mapping and integration of standards.

With R.Q. 2, we sought to discover the challenges during the mapping or integration of standards. We reasoned that the existence of challenges in these processes might indicate gaps in the literature or existing problems that should be addressed in further studies.

The goals for R.Qs. 3-5 are aligned. Our goal with these questions was to identify patterns in the use of artifacts for mapping and integrating standards, as well as the types of mapping produced through research. We also aimed to determine whether any software was used to assist in the mapping and integration processes.

**R.Q. 1** - What benefits exist from mapping or integrating standards?

**R.Q. 2** - What challenges derive from mapping or integrating standards?

**R.Q. 3** - What kinds of mappings and integrations exist for standards?

**R.Q. 4** - Which artifacts have been proposed for mapping or integrating standards...

**R.Q. 4.1** - ... at a complexity level higher than the standard's?

**R.Q. 4.2** - ... at the standard's level of complexity?

**R.Q. 4.3** - ... at a complexity level lower than the standard's?

**R.Q. 4.4** - ... utilizing software?

**R.Q. 5** - What standards have been mapped, and using which artifact?

### 3.1.3 Search Protocol

With the goal of finding all the relevant articles related to the mapping and integration of ISO/IEC standards and focusing on Risk, Security and Compliance (RSC), we carried out our search in Scopus' and ACM digital databases due to their credibility [Kitchenham, 2004].

The search string used to find the articles is: **(mapping OR integration OR integrating) AND (risk OR security OR "business continuity") AND (ISO or IEC)**. We built the string by selecting first the processes we aimed to research (Mapping and Integration), the scope of research (RSC) and the types of standards we aimed to include (ISO/IEC).

Initially, we had considered widening the scope of the SLR by removing the RSC limitation from the search string. However, this attempt resulted in the number of articles emanating from the search to increase substantially. Due to the limited number of resources in our research group, we opted to restrict the scope to our group's field of expertise.

### 3.1.4 Inclusion and Exclusion Criteria

To decide on whether to include or exclude a study from our search results, we defined a set of inclusion and exclusion criteria to guide the selection process [Kitchenham, 2004]. These criteria were defined before we began processing the articles in order to minimize researcher bias.

#### Inclusion Criteria

**Source** - Source material is a book, journal or conference proceeding

**Language** - Written in English or Portuguese

**Type** - Is a primary study or reporting on a primary study

**Field** - Is related to business continuity, risk or security

**ISO/IEC Standard** - Includes the mapping or integration of at least one ISO or IEC standard.

#### Exclusion Criteria

**Duplicate** - Article is a duplicate of another

**Accessibility** - Source not available for the full text

## 3.2 Conducting

During this stage, we executed the search strategy defined in the planning phase and identified a total of 718 papers as of the export date of 02/02/2022. Of these papers, 32 were identified as duplicates and thus removed, leaving us with 686 papers. These would be classified as "Included", "Excluded" or "Maybe" in the following step. A summary of the exclusion process can be seen in Figure 2.

### 3.2.1 Search and Selection Proceedings

After reading the titles and abstracts, we excluded 606 papers. We found that the inclusion of the term "integrating" in the search string resulted in a large number of search results related to the integration of a standard in organisations, which is clearly off-scope based on our exclusion criteria of "not mappings or integrations of two or more standards, but rather the implementation of a single one".

In the following step, we read through the introductions of the 55 "maybe" articles to decide on their inclusion or exclusion. This led to the exclusion of 49 papers and inclusion of 6.

We read the 36 included papers in full and excluded 11 more, accepting the set of the remaining 25 papers as final, presented in Table 2.

Ref	Title	Year
[Morioka, 2004]	The integrated management systems of ISO standards	2004
[Pretorius and Solms, 2004]	Information security governance using ISO 17799 and COBIT	2004

[Hoxey and Shoemaker, 2005]	Navigating the information security landscape: Mapping the relationship between ISO 15408: 1999 and ISO 17799: 2000	2005
[Von Solms, 2005]	Information Security governance: COBIT or ISO 17799 or both?	2005
[Inan et al., ]	The problems and alternative resolutions of integrated management system's implementation and sustainability: A survey on Turkish industry	2005
[Ahuja and Goldman, 2009]	Integration of COBIT, Balanced Scorecard and SSE-CMM as a strategic information security management (ISM) framework	2009
[Mas et al., 2010]	ISO/IEC 15504 best practices to facilitate ISO/IEC 27000 implementation	2010
[Magnusson and Chou, 2010]	Risk and compliance management framework for outsourced global software development	2012
[Mangin et al., 2012]	Designing a process reference model for information security management systems	2012
[Sheikhpour and Modiri, 2012]	An approach to map COBIT processes to ISO/IEC 27001 information security management controls	2012
[Beckers et al., 2013]	A method for re-using existing ITIL processes for creating an ISO 27001 ISMS process applied to a high availability video conferencing cloud scenario	2013
[Ramanauskaite et al., 2013]	Security ontology for adaptive mapping of security standards	2013
[Mesquida et al., 2014]	MIN-ITs: A framework for integration of IT management standards in mature environments	2014
[Großmann and Seehusen, 2015]	Combining security risk assessment and security testing based on standards	2015
[Rahmani et al., 2016]	CIP-UQIM: A unified model for quality improvement in software SME's based on CMMI level 2 and 3	2016
[Pardo et al., 2016b]	Towards an Integrated Management System (IMS), harmonizing the ISO/IEC 27001 and ISO/IEC 20000-2 standards	2016
[Pardo et al., 2016a]	Integrating multiple models for definition of IT governance model for banking ITGSM	2016
[Barafort et al., 2017]	Integrating risk management in IT settings from ISO standards and management systems perspectives	2017
[Muzaimi et al., 2017]	Integrated management system: The integration of ISO 9001, ISO 14001, OHSAS 18001 and ISO 31000	2017

[Ruamchat et al., 2017]	Development of quality management system under ISO 9001:2015 and Joint Inspection Group (JIG) for aviation fuelling service	2017
[Nicho, 2018]	A process model for implementing information systems security governance	2018
[Fenz and Neubauer, 2018]	Ontology-based information security compliance determination and control selection on the example of ISO 27002	2018
[Almeida et al., 2018]	A model for assessing COBIT 5 and ISO 27001 simultaneously	2018
[Almolhis and Haney, 2019]	IoT forensics pitfalls for privacy and a model for providing safeguards	2019
[Yasin et al., 2020]	Designing information security governance recommendations and roadmap using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimus Polda XYZ)	2020

Table 2: Definitions of the most relevant terms

### 3.3 Reporting

In this Subsection, we present and discuss the answers to the previously proposed research questions using information obtained from the literature.

#### 3.3.1 R.Q. 1 What benefits exist from mapping or integrating standards?

According to the literature, there are benefits from the mapping and integration of standards [Barafort et al., 2017, Beckers et al., 2013, Magnusson and Chou, 2010, Mangin et al., 2012, Mesquida et al., 2014, Muzaimi et al., 2017, Pardo et al., 2016b, Pretorius and Solms, 2004, Rahmani et al., 2016, Ramanauskaite et al., 2013, Ruamchat et al., 2017, Sheikhpour and Modiri, 2012, Solms, 2005, Yasin et al., 2020]. A large part of these benefits are based on improved access and quality of information [Pretorius and Solms, 2004, Ramanauskaite et al., 2013], allowing for more efficient communication of information. A summary of these benefits can be found in Table 3.

Mappings can help bridge the gap between different areas of expertise [Magnusson and Chou, 2010, Pretorius and Solms, 2004, Solms, 2005]. For example, the literature proposes that the gap between Governance and Information Technology can be bridged through a mapping between ISO 27002 and COBIT's DS 5 - *Ensure Systems Security help* [Pretorius and Solms, 2004, Solms, 2005], with the ISO standard presenting the "how" (the technical aspects at a lower level) and COBIT the "why/what" (the higher level, governance-side aspects). This is especially helpful since it improves communication, reusability and organization of knowledge [Ramanauskaite et al., 2013].

In addition to a more efficient flow of information, compliance to laws, policies and standards is also shown to be significantly improved with the mapping and integration of standards [Beckers et al., 2013, Magnusson and Chou, 2010, Muzaimi et al., 2017,



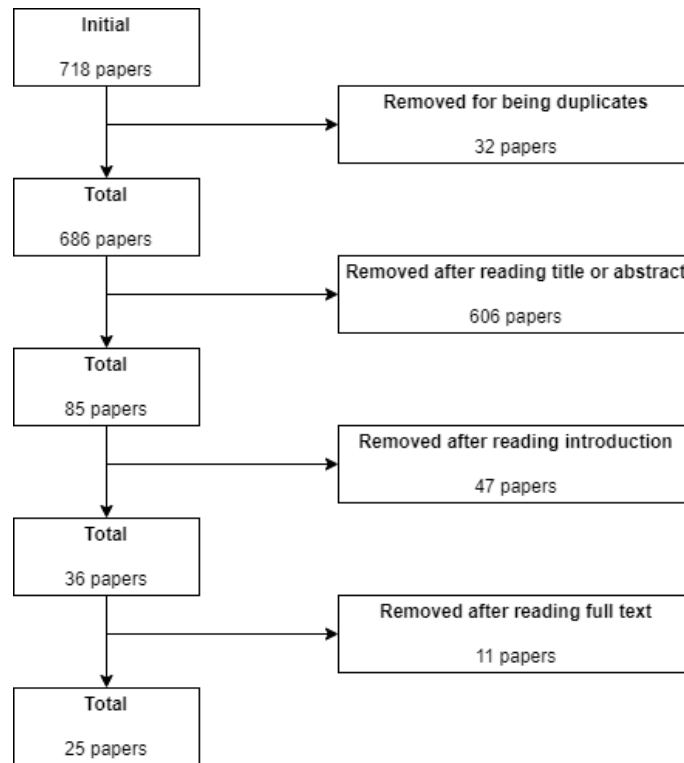


Figure 2: Summary of the selection process

Pretorius and Solms, 2004, Ruamchat et al., 2017, Solms, 2005]. There are two main improvements that lead to this benefit:

- **Easier implementation** - By having all the information of what controls need to be implemented in one single artifact, enterprises have an easier time determining what controls have already been implemented and maintained [Magnusson and Chou, 2010].
- **Better auditing** - Auditing is another essential aspect of compliance [Vroom and Von Solms, 2004] that can be improved by the mapping and integration of standards. The literature shows that it is easier for auditors to validate compliance [Muzaimi et al., 2017, Pretorius and Solms, 2004, Ruamchat et al., 2017], leading to better law compliance [Magnusson and Chou, 2010] and reduced costs from more efficient use of internal auditors' time [Mesquida et al., 2014].

We have found evidence that indicates that Risk Management is another area that benefits from the mapping and integration of standards [Pardo et al., 2016b], often through the mitigation of risks, causing a reduction in the number of incidents across the same timeframe [Ruamchat et al., 2017].

The literature also provides evidence that the business itself can benefit from the mapping and integration of standards. Certification is easier to attain [Mangin et al.,

	Better Auditing and Compliance	Improved Cooperation	Improved Risk Management	Higher Efficiency	Easier Standard Adoption
[Muzaimi et al., 2017]	X	X	X	X	X
[Pretorius and Solms, 2004]	X	X			
[Solms, 2005]	X	X			
[Ruamchat et al., 2017]	X		X		
[Beckers et al., 2013]	X				X
[Magnusson and Chou, 2010]	X				X
[Ramanauskaite et al., 2013]		X			
[Almeida et al., 2018]		X			
[Pardo et al., 2016b]			X		
[Sheikhpour and Modiri, 2012]			X	X	
[Yasin et al., 2020]				X	
[Mesquida et al., 2014]					X
[Rahmani et al., 2016]					X
[Mangin et al., 2012]					X

Table 3: Summary of the most relevant benefits across the literature

2012, Muzaimi et al., 2017], primarily when one of the mapped standards has already been implemented [Rahmani et al., 2016].

Moreover, organizations can observe improved public image through the implemented certifications [Mesquida et al., 2014] and transparency [Yasin et al., 2020], making it easier to attract new customers or improve the loyalty of existing ones [Muzaimi et al., 2017].

### 3.3.2 R.Q. 2 What challenges arise from mapping or integrating standards?

The literature presents a sizable lack of information regarding the challenges present in the process of mapping or integrating standards. We believe that is due to a lack of systematic reporting, leading to the articles being entirely focused on presenting the results of their findings and not so much on the process used.

The few challenges found are mainly related to the artifact used to map the standards, making it hard to derive generalizations from the literature. However, we can say that mapping standards is often a very time-consuming process. Most mapping methods involve multiple review sessions where researchers meet, discuss ideas, and share knowledge to improve upon the proceedings of the previous meetings [Mas et al., 2010].

Taking a look at a specific artifact, ontologies, we can deduce that it is often impossible to map onto them bi-directionally with relative term accuracy. Comprehensive ontologies include terms from multiple standards and as such, will not be able to be fully mapped back onto a single standard. Thus, one must make a choice between bi-directionality of the mapping and coverage of terms on the ontology, which can be a challenge on its own [Ramanauskaite et al., 2013].

One other challenge that we inferred from the literature, which is not directly presented in the articles, is that the mapping and integration processes can be highly resource-intensive, using up a significant portion of a research group's time [Ruamchat et al., 2017].

### 3.3.3 R.Q. 3 What kinds of mappings and integrations exist for standards?

The literature does not present different kinds of integrations. However, every integration requires a mapping to be done beforehand. Thus, we are only considering mappings to answer this question as the answers given also apply to the mapping stage of integrations. To assist in understanding and responding to this research question, we bring to light two distinct concepts, i.e., abstraction level and directionality:

**Abstraction level** - mappings can engulf concepts at different abstraction levels and as such, the relationships between elements can change. It is possible to map a single control to many [Pretorius and Solms, 2004], or many controls to one [Ramanauskaite et al., 2013], as is usually the case with ontologies [Fenz and Neubauer, 2018, Ramanauskaite et al., 2013]. It is also possible to map elements other than controls, including categories or processes, provided that all of their lower level controls are mapped to [Mas et al., 2010].

**Directionality** - Unidirectional mappings present a one-way map: corresponding the terms of one standard to terms of another, but not the opposite. This property leads to more straightforward mappings by reducing artifact sizes, but cuts some use cases. Bi-directional mappings encompass all use cases by ensuring that either standard is both source and destination and allowing elements to be mapped starting from any of its mapped standards. In some cases, researchers claim that it is trivial to extend a unidirectional mapping by retracing its steps [Pretorius and Solms, 2004].

### 3.3.4 R.Q. 4 Which artifacts are used/have been proposed for mapping or integrating ISO/IEC standards?

We decided to assign each of the artifacts proposed in the literature to one of four groups, based on the complexity of the artifact: Group 1 - Construct (frameworks, ontologies, metamodels) Group 2 - Model Group 3 - Method/Algorithm Group 4 - Software (automated)

In Group 1, we discovered two frameworks: SABSA [Magnusson and Chou, 2010] and HFramework [Rahmani et al., 2016] and two unnamed security ontologies [Fenz and Neubauer, 2018, Ramanauskaite et al., 2013]. These generally aim to generalize and map standards onto them. The ontologies have great coverage of the standards they aim to span.

In Group 2, we found some models created by researchers to map standards [Almeida et al., 2018, Barafort et al., 2017], specifically, Process Reference Models (PRMs) have been used to map atomic requirements in a stricter way [Mangin et al., 2012].

Group 3 presents methods with less formality than the previous groups, replacing the well-defined (meta)models with an algorithm or list of methods. Some follow stricter guidelines like [Beckers et al., 2013, Mas et al., 2010], others a more lenient approach, using a sequential list of strategies [Pardo et al., 2016b].

Group 4 represents entries related to mappings and integrations deriving from software, but we have not found any in the literature.

### 3.3.5 R.Q. 5 What standards have been mapped and using which artifact?

We identified that ISO 27000 comprised most of the mappings and integrations using ISO standards, amounting to 54% of the total identified mappings and 33% of integrations.

Below, in Tables 4 and 5, we present the most commonly mapped (Table 4) and integrated (Table 5) standards and which group of artifacts they were processed with.

The groups were defined in the same manner and logic as in R.Q. 4. In the columns, we list the aforementioned groups of artifacts, and in the rows the most common standards. It is worth noting that we grouped the entire family of ISO 27000 standards into a single row (ISO 2700X), including ISO 27001, 27002 and 17799.

<b>Mapping</b>	Construct	Model	Method	Software	<b>Total</b>
ISO 2700X	3	4	5	0	12
ISO 20000	0	2	1	0	3
ISO 15504	0	0	1	0	1
ISO 9001	0	1	0	0	1
COBIT	0	3	2	0	5
<b>Total</b>	3	10	9	0	22

*Table 4: Most relevant mapping data*

<b>Integration</b>	Construct	Model	Method	Software	<b>Total</b>
ISO 2700X	1	1	0	0	2
ISO 20000	1	1	0	0	2
ISO 15504	0	1	0	0	1
ISO 9001	0	1	0	0	1
COBIT	0	0	0	0	0
<b>Total</b>	2	4	0	0	6

*Table 5: Most relevant integration data*

From the data, we can gather that there is a significant interest in the ISO 2700X family of standards, spanning over half of the mappings and a third of all integrations. COBIT also appeared in a large amount of mappings despite not being explicitly included in the search.

Apart from that, we can also conclude that around half of the authors opted for formal mapping and integration methods, using constructs and models, while the other half preferred less formal methods. It is also worth noting that no mappings or integrations utilized software to automate processes.

## 4 Discussion

After having reported the SLR's results, in this section, we analyse and discuss them in further detail.

We have found the mapping and integration of ISO/IEC standards to be very beneficial processes for organizational development. They make it easier for organizations to adopt new standards, while improving compliance mechanisms and reducing implementation costs.

The SLR has also shown that these benefits come at a cost: the mapping process is very time-intensive, which can be a problem in some resource-constrained situations, since a group of researchers is required to iteratively meet and discuss which parts of each standard can be mapped. The results of these discussions are then analyzed and, from them, a mapping artifact is generated.

To compound this problem, the intermediate information (i.e., the thought process, the notes taken) generated during the mapping process is not backward-traceable from the artifact and is generally not reported on. Thus, if changes are required, the artifact will have to be redone through the same time-consuming process.

Changes to standards' mappings can originate from a few different sources. Below we explore some of the possible reasons that can lead to the redoing of parts of a mapping or integration.

- **Revision** - Standards are often revised and updated. Sometimes these revisions can cause major changes to the controls or structure
- **Directionality** - It is possible to create a directional mapping, but leave open the possibility of making it bi-directional in the future
- **Scalability** - Most of the mappings and integrations found in the literature included only two standards, but it is possible to expand them to more.

Seeing that any two standards can be mapped, provided that there are some common points between them, one can deduce the sheer magnitude of combinations that can be formed involving ISO standards. This means that it is not feasible to map every combination of standards manually, due to how time-consuming it would be to create and maintain the artifacts.

There are numerous different methods of achieving the same mapping (and possibly integration) [Mas et al., 2010] with two or more standards. Moreover, despite the results of these processes being very beneficial, there is not a standardized way to map or integrate standards. We believe it would be useful for organizations to know what would be the best approach of adapting their systems into being compliant with a new standard or certification.

We have found the majority of mappings to take an iterative design approach. With meeting after meeting, the mappers share ideas and discuss on each control's relation to another. This can be repeated among different research groups to achieve less bias or simply have everyone discuss in a "round-table" approach. We do not see this as a scalable process, for it has to be repeated every time a new standard is mapped, resulting in massive time consumption.

Some works utilize computer assistance [Pretorius and Solms, 2004, Solms, 2005], but only as a database provider. In addition, these studies predate all the others by five years, making them reasonably outdated as of this paper's writing. Moreover, the authors are reporting on a mapping from ISO 17799 to COBIT, the former of which is not only outdated, but also "defunct", having been replaced by the newer ISO 27002, that is the set of guidelines of the certifiable ISO 27001 for Information Security.

To summarize, we argue that current methods of generating mapping artifacts are not only cumbersome to execute, but also ineffective as they output a single artifact without the reasoning behind it. This makes future changes to the mapping more complicated, since the original thought process behind each control's mapping is not reported.

The literature also does not present any software-based harmonization, mapping or integration assistance (or automation) tool to automate some of the time-consuming

parts of these processes. Since such parts are often repetitive, the authors consider the automation of certain processes to be plausible.

## 5 Conclusion

In this paper, we conducted an SLR to study the impacts, challenges and artifacts deriving from the mapping and integration of ISO/IEC standards. The SLR has raised the state of the art over the topic of Mapping and Integration of ISO and IEC standards related to security, risk and business continuity.

We applied our inclusion and exclusion criteria over the 718 papers discovered, leaving us with 25 relevant primary studies, which we read and analysed.

We conclude that the mapping and integration of standards bring a large number of benefits, ranging from better risk management and easier compliance to business-side benefits like reduced costs, ease of certification and better business image.

During the review of the SLR's data, we have also identified some challenges arising from both the mapping and integration of standards. The main problem we discovered was the resource intensity of the mapping and integration processes over two or more standards. This problem is compounded by other human factors, for example, any language barrier that exists in the research teams leads to more time being spent. Additionally, when mapping to ontologies, it is necessary to choose between bi-directionality or bigger coverage of the mapping.

There are some limitations to our paper, the first being that we only searched for articles in two databases, i.e., Scopus and ACM. Although they are considered credible sources of information [Kitchenham, 2004], it could be helpful to include other sources of scientific articles in further research. Moreover, we have only studied mappings and integrations over ISO/IEC standards, leaving out all of the mappings and integrations that do not include at least one ISO/IEC standard.

For future work, we have identified a possible path of research to improve the processes for mapping and integrating standards. There exists a large research gap concerning the use of software tools in a hybrid or partially-automated approach to assist in the mapping of ISO and IEC standards.

Based on our assessments, we believe that automating some of the processes within the harmonization and mapping of standards could speed up these processes by a significant amount. Information Retrieval techniques could be applied to extract the controls from standards and find intersections between clauses of different standards.

## References

- [Ahuja and Goldman, 2009] Ahuja, S. and Goldman, J. (2009). Integration of cobit, balanced scorecard and sse-cmm as a strategic information security management (ism) framework. *College of Technology, Purdue University, West Lafayette*.
- [Almeida et al., 2018] Almeida, R., Lourinho, R., Silva, M. M. D., and Pereira, R. (2018). A model for assessing cobit 5 and iso 27001 simultaneously. 1:60–69.
- [Almolhis and Haney, 2019] Almolhis, N. and Haney, M. (2019). Iot forensics pitfalls for privacy and a model for providing safeguards. In *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, pages 172–178. IEEE.

- [Barafort et al., 2017] Barafort, B., Mesquida, A.-L., and Mas, A. (2017). Integrating risk management in it settings from iso standards and management systems perspectives. *Computer Standards and Interfaces*, 54:176–185.
- [Beckers et al., 2013] Beckers, K., Hofbauer, S., Quirchmayr, G., and Wills, C. C. (2013). A method for re-using existing itil processes for creating an iso 27001 isms process applied to a high availability video conferencing cloud scenario. 8127:224–239.
- [Castillo-Rojas et al., 2012] Castillo-Rojas, S. M., Casadesús, M., Karapetrovic, S., Coromina, L., Heras, I., and Martín, I. (2012). Is implementing multiple management system standards a hindrance to innovation? *Total Quality Management & Business Excellence*, 23(9-10):1075–1088.
- [Fenz and Neubauer, 2018] Fenz, S. and Neubauer, T. (2018). Ontology-based information security compliance determination and control selection on the example of iso 27002. *Information & Computer Security*.
- [Großmann and Seehusen, 2015] Großmann, J. and Seehusen, F. (2015). Combining security risk assessment and security testing based on standards. In *Risk Assessment and Risk-Driven Testing: Third International Workshop, RISK 2015, Berlin, Germany, June 15, 2015. Revised Selected Papers 3*, pages 18–33. Springer.
- [Gunawan et al., 2020] Gunawan, N. K., Hadiprakoso, R. B., and Kabetta, H. (2020). Comparative study between the integration of itil and iso/iec 27001 with the integration of cobit and iso/iec 27001. In *IOP Conference Series: Materials Science and Engineering*, volume 852, page 012128. IOP Publishing.
- [Hoxey and Shoemaker, 2005] Hoxey, C. and Shoemaker, D. (2005). Navigating the information security landscape: Mapping the relationship between iso 15408: 1999 and iso 17799: 2000.
- [Inan et al., ] Inan, U. H., Baraçlı, H., and Çetinsaya, V. The problems and alternative resolutions of integrated management system’s implementation and sustainability: A survey on turkish industry.
- [ISO/IEC 27001:2013, 2000] ISO/IEC 27001:2013 (2000). Information security management. Standard, International Organization for Standardization, Geneva, CH.
- [IT Governance Institute, 2007] IT Governance Institute, editor (2007). *CobIT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models*. IT Governance Institute, Rolling Meadows.
- [Keele et al., 2007] Keele, S. et al. (2007). Guidelines for performing systematic literature reviews in software engineering. Technical report, Technical report, Ver. 2.3 EBSE Technical Report. EBSE.
- [Kitchenham, 2004] Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33(2004):1–26.
- [Lopes et al., 2019] Lopes, I. M., Guarda, T., and Oliveira, P. (2019). How iso 27001 can help achieve gdpr compliance. In *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–6. IEEE.
- [Magnusson and Chou, 2010] Magnusson, C. and Chou, S.-C. (2010). Risk and compliance management framework for outsourced global software development. *Proceedings - 5th International Conference on Global Software Engineering, ICGSE 2010*, pages 228–233.
- [Mangin et al., 2012] Mangin, O., Barafort, B., Heymans, P., and Dubois, E. (2012). Designing a process reference model for information security management systems. 290:129–140.
- [Mas et al., 2010] Mas, A., Mesquida, A. L., Amengual, E., and Fluxà, B. (2010). Iso/iec 15504 best practices to facilitate iso/iec 27000 implementation. pages 192–198.
- [Mesquida et al., 2014] Mesquida, A.-L., Mas, A., Feliu, T. S., and Arcilla, M. (2014). Min-its: A framework for integration of it management standards in mature environments. *International Journal of Software Engineering and Knowledge Engineering*, 24:887–908.

- [Morioka, 2004] Morioka, T. (2004). The integrated management systems of iso standards. *Journal of global environment engineering*, 10:215–224.
- [Mussmann et al., 2020] Mussmann, A., Brunner, M., and Brey, R. (2020). Mapping the state of security standards mappings. In *Wirtschaftsinformatik (zentrale tracks)*, pages 1309–1324.
- [Muzaimi et al., 2017] Muzaimi, H., Chew, B. C., and Hamid, S. R. (2017). Integrated management system: The integration of iso 9001, iso 14001, ohsas 18001 and iso 31000. 1818.
- [Nicho, 2018] Nicho, M. (2018). A process model for implementing information systems security governance. *Information & Computer Security*, 26(1):10–38.
- [Pardo et al., 2016a] Pardo, C., Garcia, F., Piattini, M., Pino, F. J., Lemus, S., Baldassarre, M. T., et al. (2016a). Integrating multiple models for definition of it governance model for banking itgsm. *International Business Management*, 10(19):4644–4652.
- [Pardo et al., 2016b] Pardo, C., Pino, F. J., and Garcia, F. (2016b). Towards an integrated management system (ims), harmonizing the iso/iec 27001 and iso/iec 20000-2 standards. *International Journal of Software Engineering and its Applications*, 10:217–230.
- [Pardo et al., 2012] Pardo, C., Pino, F. J., Garcia, F., Piattini, M., and Baldassarre, M. T. (2012). An ontology for the harmonization of multiple standards and models. *Computer Standards & Interfaces*, 34(1):48–59.
- [Pretorius and Solms, 2004] Pretorius, E. and Solms, B. V. (2004). Information security governance using iso 17799 and cobit. 140:107–113.
- [Rahmani et al., 2016] Rahmani, H., Sami, A., and Khalili, A. (2016). Cip-uqim: A unified model for quality improvement in software sme's based on cmmi level 2 and 3. *Information and Software Technology*, 71:27–57.
- [Ramanauskaite et al., 2013] Ramanauskaite, S., Olifer, D., Goranin, N., and Čenys, A. (2013). Security ontology for adaptive mapping of security standards. *International Journal of Computers, Communications and Control*, 8:878–890.
- [Ritchie and Brindley, 2007] Ritchie, B. and Brindley, C. (2007). Supply chain risk management and performance: A guiding framework for future development. *International Journal of Operations & Production Management*.
- [Ruamchat et al., 2017] Ruamchat, K., Thawesaengkulthai, N., and Pongpanich, C. (2017). Development of quality management system under iso 9001:2015 and joint inspection group (jig) for aviation fuelling service. *Management and Production Engineering Review*, 8:50–59.
- [Sandadi, 2017] Sandadi, R. (2017). *ITIL Foundation Reference Guide: Concepts, Use Case, Exam Guide*. Independently published.
- [Sheikhpour and Modiri, 2012] Sheikhpour, R. and Modiri, N. (2012). An approach to map cobit processes to iso/iec 27001 information security management controls. *International Journal of Security and Its Applications*, 6(2):13–28.
- [Simon et al., 2012] Simon, A., Karapetrovic, S., and Casadesús, M. (2012). Difficulties and benefits of integrated management systems. *Industrial Management & Data Systems*.
- [Solms, 2005] Solms, B. V. (2005). Information security governance: Cobit or iso 17799 or both? *Computers and Security*, 24:99–104.
- [Von Solms, 2005] Von Solms, B. (2005). Information security governance: Cobit or iso 17799 or both? *Computers & Security*, 24(2):99–104.
- [Vroom and Von Solms, 2004] Vroom, C. and Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & security*, 23(3):191–198.
- [Yasin et al., 2020] Yasin, M., Akhmad Arman, A., Edward, I. J. M., and Shalannanda, W. (2020). Designing information security governance recommendations and roadmap using cobit 2019 framework and iso 27001:2013 (case study ditreskrimsus polda xyz). pages 1–5.