Enterprise Risk Management and Information Systems: a Systematic Literature Review

Andre D. Fernandes
Daniel Ramalho
Miguel Mira da Silva

Follow this and additional works at: https://aisel.aisnet.org/confirm2022

This material is brought to you by the International Conference on Information Resources Management (CONF-IRM) at AIS Electronic Library (AISeL). It has been accepted for inclusion in CONF-IRM 2022 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Andre D Fernandes
Universidade de Lisboa
andre.fernandes@inov.pt

Daniel Ramalho
Universidade de Lisboa
daniel.ramalho@tecnico.ulisboa.pt

Miguel Mira Da Silva
Universidade de Lisboa
mms@tecnico.ulisboa.pt

Abstract

Enterprise Risk Management (ERM) aims to help organizations better monitor, analyze, and control their risks and policymakers to focus on procedures to improve organization and risk governance. Over the years, several artifacts have been proposed in this area to address different goals in ERM. The main objective of this article is to provide an overview of the literature related to the areas of ERM and Information Systems in order to understand how traditional risk governance adapts to the new digital reality of organizations. To better structure the results obtained, the articles were divided into three distinct categories: articles that offer guidelines for ERM management, articles that propose ways to measure the maturity of organizations in ERM, and articles that propose methods to increase an organization's maturity in ERM.

Keywords: Enterprise Risk Management, ERM, Systematic Literature Review, Framework.

1. Introduction

Risk is a concept used in several domains and does not have a single definition (Janney and Dess 2006). Enterprise Risk Management (ERM) is a derivative of traditional risk management that aims to model, monitor, evaluate, and respond to organizations' risks (Gordon, Loeb, and Tseng 2009). ERM “allows/helps/enables/supports organizations in achieving their performance and profit targets and prevent resource loss” (COSO 2017).

As an essential part of ERM, enterprise risk analysis has been extensively developed by academics and practitioners (Oliva 2016), resulting in the development of different artifacts that aim to integrate the risk assessment into organizational cultures and, thereafter, the inclusion of risk management in the list of enterprises’ organizational processes (COSO 2017; Purdy 2010; RIMS 2006). The COSO and ISO 31000 frameworks are examples of structured approaches for organizations to manage ERM efficiently (COSO 2017; ISO 31000).

Given the broadness of the ERM field and the variety of possible solutions in different scientific articles, we conducted a literature review to analyze the proposed solutions for ERM management. To the best of our knowledge, no existing article presents the state-of-the-art frameworks, models, and methods currently under development and implemented to help organizations manage ER, either by the industry or the scientific community. We want to point out that the work of (Anton and Nucu 2020) makes a unique summary of the topics covered in the ERM literature, but does not answer the questions we proposed. This article provides a structural overview of ERM management by categorizing existing research works based on a Systematic Literature Review (Kitchenham et al., 2009).
Nowadays, many organizations depend on information systems to be or become competitive in their field of competence. The technological element of organizations makes them vulnerable to natural and human-made threats, whose outcomes are highly unpredictable (Jovanović, Renn, and Schröter 2012). However, the authors are unaware of any research that considers linking the theoretical domains of IT Governance and ERM. Thus, in this SLR, all the selected articles considered the area of information systems in their domain or are abstract enough to encompass this area.

The paper is structured as follows: Section 2 describes the research methodology, the plan and the execution of the SLR. In Section 3, the Research Questions and the research results are reported. Section 4 concludes this article.

2. Systematic Literature Review

A Systematic Literature Review (SLR) is a methodology that provides a systematic and rigorous process for reviewing and analyzing the literature, identifying, analyzing, and interpreting all available materials in a particular domain (Kitchenham et al. 2009). An SLR consists of three stages:

- **Planning** – the research questions, SLR goals, and exclusion and inclusion criteria are defined, and a review process is written.
- **Conducting** – the articles are collected, organized and filtered using the process defined in the previous step.
- **Reporting** – the extracted information from the selected studies is summarized and the research questions are answered.

2.1 Planning phase

In this phase, the execution process of the SLR was designed. To this end, the research questions were established, the databases to be used were chosen, the search string to find relevant articles was defined and the inclusion and exclusion criteria to filter the articles were defined.

2.1.1 Research Questions

This research explores the contents of existing studies published in the ERM domain, specifically to understand what kinds of options, in terms of models and frameworks, are available for organizations to implement, assess and improve their ERM processes. For this purpose, we defined the following Research Questions (RQ):

- **RQ1** - What frameworks are being used in the ERM domain?
- **RQ2** - What assessment models are being used to assess ERM maturity?
- **RQ3** - What methods are being used to increase maturity in ERM?
  - **RQ3.1** - Which steps of risk management receive more attention?
- **RQ4** - What are the foundations used for the work?
  - **RQ4.1** - Are they based on existing standards?
  - **RQ4.2** – What conceptual models are being used or proposed?

The paper aims to attain a comprehensive view of the solutions proposed in the literature in recent years. Therefore, three macro questions were formulated, representing the three main vectors of analysis that were considered in this research: managing, assessing and improving ERM. The fourth vector of analysis, concerning the foundations of the works, has been added to understand the underlying basis of what was proposed.
2.1.2 Search Process

Five different databases were used in our search process to obtain a comprehensive set of publications for this research:

- EBSCO Host (http://eds.b.ebscohost.com/)
- SCOPUS (http://www.scopus.com)
- ACM Digital Library (http://portal.acm.org)
- Web of Science (http://www.isiknowledge.com)
- IEEE Xplore (http://ieeexplore.ieee.org)

The results were obtained by using a standard search string encompassing both the Title and Abstract. The articles were collected from the different databases in March 2022.

Table 1: Generic Search String

<table>
<thead>
<tr>
<th>Search String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title (Risk AND (manage* OR erm) AND (model* OR framework OR method*)) AND Abstract ((process OR maturity OR capability) AND (digital OR info* OR software) AND (assess* OR eval* OR manage*))</td>
</tr>
</tbody>
</table>

2.1.3 Inclusion and Exclusion Criteria

To extract relevant publications for the research, a set of Inclusion Criteria (IC) and Exclusion Criteria (EC) were defined, as recommended by (Kitchenham et al. 2009).

- EC1: Articles published in 2010 or earlier
- EC2: Articles not written in the English language
- EC3: Publications not from scientific journals or conferences
- EC4: Surveys or educational articles
- EC5: National policies
- EC6: Articles focused only on a specific business field (e.g., civil construction, health, environment)
- EC7: Articles lacking peer review
- EC8: Duplicated articles (prioritizing the more complete and recent versions)
- IC1: Indexed conference or journal
- IC2: Articles focused on best practices, frameworks, models, taxonomies, and processes in the ERM domain

2.2 Search Process

The publications were identified by searching through databases of academic publications using the predefined search string (Table 1). After the articles were collected from the different databases, they were all centralized using the Rayyan tool (https://rayyan.qcri.org/).

The first step in this process was the removal of duplicate articles. Then, the screening phase was initiated, where the titles and abstracts of the remaining articles were read and the articles were classified, according to the predefined inclusion and exclusion criteria, into three categories: "Include", "Maybe" and "Exclude". The articles classified as “Include” automatically proceeded to the next process phase. The articles classified as “Exclude” were labeled with the criteria they violated to justify their exclusion. The articles classified as “Maybe” were analyzed in more detail and discussed among the authors until a consensus was reached on whether it should be included or excluded. The Scimago ranking (https://www.scimagojr.com/) and the Core (http://portal.core.edu.au) were consulted for the
journals’ and conferences’ rankings. Articles published in conferences or journals that were not listed in any of these rankings were eliminated from the research.

In the next phase, the articles' introductions and conclusions were read and the articles were again classified and filtered as in the screening phase. The remaining articles were then fully read, classified, and filtered as in the previous phases. In the end, thirty articles were accepted and later analyzed and classified into different categories, as shown in the following sections. The process is summarized in Error! Reference source not found..

### 2.2.1 Classification Scheme
Categories were defined to classify the articles during the screening phase in order to make their analysis clearer and more efficient. The classification process started in the screening phase and ended after the complete analysis of the articles. This process was iterative and discussed among the authors. In the end, all articles were classified according to the type of artifact created and whether validation was performed in their research. The types of solutions are explained in Section 3.

### 3. Discussion
A series of parameters were selected to analyze and categorize the articles based on the classification scheme process in order to answer the Research Questions. All articles were classified according to the type of their contribution and whether or not it was validated. Error! Reference source not found. shows the categories created to classify the articles. Articles were considered validated if they used any method (case studies, interviews, etc.) to validate their solution with real organizations or real-world scenarios. However, some articles in this category were classified as “Exemplified” as they used fictitious organizations or data to validate their research. Those classified as non-validated did not meet any of these criteria. The solution column summarize the artifacts presented in each of the articles. One nuance is present in Error! Reference source not found. in the form of the Framework* label. These articles consist of high-level, general guidelines, like common frameworks, but instead of guiding ERM directly, they guide the adoption or implementation of other pre-existing frameworks or standards.
Figure 1 Article selection and filtering process.

<table>
<thead>
<tr>
<th>Type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment Model</td>
<td>The paper provides a model or significantly modifies an existing model for assessing the capability of processes or the maturity of organizations concerning the ERM domain.</td>
</tr>
<tr>
<td>Framework</td>
<td>The article provides a structured list of processes, guidelines or best practices designed for organizations in the ERM domain.</td>
</tr>
<tr>
<td>Method</td>
<td>The paper proposes solutions that fully or partially improve processes within the ERM domain.</td>
</tr>
<tr>
<td>Opinion Paper</td>
<td>The paper does not propose something new (assessment model, framework, or method) but rather analyzes and draws conclusions about certain concepts or solutions</td>
</tr>
<tr>
<td>Conceptual Model</td>
<td>The paper presents a model to represent concepts and/or relationships in the ERM domain.</td>
</tr>
<tr>
<td>Implementation</td>
<td>The article focuses on the implementation of frameworks in organizations</td>
</tr>
<tr>
<td>Reference</td>
<td>Type</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>(Webb et al. 2014)</td>
<td>Assessment Model</td>
</tr>
<tr>
<td>(Javaid and Iqbal 2017)</td>
<td>Framework*</td>
</tr>
<tr>
<td>(Deshpande and Desai 2021)</td>
<td>Framework</td>
</tr>
<tr>
<td>(Khosravi-Farmad and Ghaemi-Bafghi 2020)</td>
<td>Framework</td>
</tr>
<tr>
<td>(Ntouskas and Polemi 2012)</td>
<td>Framework</td>
</tr>
<tr>
<td>(Chen 2011)</td>
<td>Method</td>
</tr>
<tr>
<td>(Spremic 2012)</td>
<td>Method</td>
</tr>
<tr>
<td>(Suyasa and Legowo 2019)</td>
<td>Implementatio n</td>
</tr>
<tr>
<td>(Lee 2021)</td>
<td>Framework</td>
</tr>
<tr>
<td>(Flores and Morocho 2020)</td>
<td>Framework</td>
</tr>
<tr>
<td>Source</td>
<td>Type</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>(Ganin et al. 2020)</td>
<td>Assessment Model</td>
</tr>
<tr>
<td>(Saleh and Alfantoorkh 2011)</td>
<td>Framework</td>
</tr>
<tr>
<td>(Thalmann et al. 2014)</td>
<td>Framework</td>
</tr>
<tr>
<td>(Huang et al. 2011)</td>
<td>Method</td>
</tr>
<tr>
<td>(Ali, Warren, and Mathiassen 2017)</td>
<td>Framework</td>
</tr>
<tr>
<td>(Meng 2013)</td>
<td>Implementation</td>
</tr>
<tr>
<td>(Maneerattanasak and Wongpinunwatana 2017)</td>
<td>Framework</td>
</tr>
<tr>
<td>(Torabi, Giahi, and Sahebjamnia 2016)</td>
<td>Framework</td>
</tr>
<tr>
<td>(Kohnke, Sigler, and Shoemaker 2016)</td>
<td>Opinion Paper</td>
</tr>
<tr>
<td>(Khrisna and Harlili 2015)</td>
<td>Framework</td>
</tr>
</tbody>
</table>
The research questions RQ1, RQ2 and RQ3 are answered in Table 3, where the articles are classified according to the previously defined scheme. Although the number of articles was insufficient to identify trends, we extracted all algorithms used in the research and performed a time-based analysis, as shown in Figure 2. It is possible to verify that OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) and Multi-Criteria Decision Making (MCDM) algorithms (Fuzzy and AHP) have been constantly referenced in the literature over the years. In the case of Bayesian methods, we speculate that the growing interest in the area of artificial intelligence was responsible for the peak in 2020. To answer question RQ3.1, the articles classified as "Methods" were analyzed to identify the phases in which the method operates. The articles that present methods are summarized in Table 4.
### Table 4 Summary of articles classified as Method.

<table>
<thead>
<tr>
<th>Paper</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chen (2011)</td>
<td>Inserts Bohem’s spiral model into the Risk Management process to introduce constant, iterative actions that encourages systematic improvement. This method can be considered holistic as it covers the entire process of Risk Management.</td>
</tr>
<tr>
<td>Huang et al. (2011)</td>
<td>The proposal serves to improve the Evaluation of Governance Controls. The list of objectives that they construct covers a wide variety of issues in an organization, including explicit processes for Risk Identification, Risk Assessment, Risk Response, and general monitoring and management.</td>
</tr>
<tr>
<td>Anikin (2015)</td>
<td>The solution aims to improve the Vulnerability Risk Assessment process, based on the Common Vulnerability Scoring System proposed by NIST and Carnegie Mellon University. Those results are then combined with Threat Impact and Possibility metrics to obtain a Risk Assessment.</td>
</tr>
<tr>
<td>Spremić (2012)</td>
<td>Frames the solution in terms of Corporate IT Risk Management and elaborates a plan based on the literature to improve the Risk Identification and Risk Assessment processes.</td>
</tr>
</tbody>
</table>

To answer RQ4 and subsequently RQ4.1 and RQ4.2, the standards and taxonomies used by the collected articles were identified, as shown in Error! Reference source not found.. Many articles involve literature reviews on the area and solid related work sections. We make the following comment, not only on the articles collected but also on those that were fully read but removed in the last phase:

- ISO standards were one of the most often-used references. The ISO 27XXX standard family was used consistently throughout the timeframe, with ISO 27001 being the most constant. The PDCA Model from this standard was particularly emphasized. The ISO 31XXX standard family was referenced, but we expected that this would undoubtedly be the most used given its interconnection with the scope of this research. ISO 22301 was also mentioned, but not frequent enough to discern any patterns.

- We also expected more frequent reference to frameworks such as COBIT and ITIL, given that this research required that articles consider the IT Governance domain.

In the case of RQ4.2, we only identified one article (Mayer et al., 2019) that modeled ERM concepts using a modeling language (ArchiMate). We consider this kind of article essential to establish foundations, as throughout this research, we noticed some lack of consistency concerning concepts and definitions, for example, the inaccurate usage of certain concepts. This type of article may also help resolve inconsistencies found in ERM and Project Risk Management as they share similar concepts.

After collecting and classifying all articles, we realized the final number of publications was too low. We concluded that this area is still relatively young and lacks specialization in particular areas, more specifically in ERM governance. We expected a more significant link to industry-recognized standards (e.g., ISO 31000, COBIT). We want to highlight the lack of research into the link between IT Governance and ERM. In our opinion, this is a possible area to be explored in the future, given the complexity and dependency that organizations have on information systems. During the research, we noticed a significant focus on Project Risk Management, given that a large percentage of the articles eliminated in the different phases were from this domain.
4. Conclusion

In this paper, an SLR was performed to analyze the existing literature on ERM frameworks, assessment models and methods. This research answered four research questions about the existing research literature. A total of 30 publications were analyzed and classified, helping to clarify what is being researched in terms of best practices, models to assess ERM and methods to improve organizations in this area, and also determining what the most influential and significantly used artifacts are in this field.

In addition to the articles' classification as methods, frameworks, opinion papers, or assessment models, the integration with standards was also presented. This research attempted to identify conceptual models that clearly define the area of ERM, but only one relevant article was found, which might indicate a lack of attention towards this aspect in the literature. On the other hand, 15 of the 30 articles were classified as frameworks, indicating that this type of solution has received the most attention.

Our research leads us to conclude that the lack of ERM research and a potential enhancement by including IT Governance highlight an opportunity for future research. We also observed a strong focus on the risk assessment processes in the literature compared to other risk areas.

Even though this research follows the proper procedures suggested by the literature, there are nevertheless some major limitations. The number of articles is not exceptionally high and therefore, snowballing techniques could not be applied to increase the final number of articles. Although the low number of articles found can be justified by the fact that the areas of ERM and IT Governance are only recently being formally connected, this inevitably leads to limited statistical analysis. As future work, we recommend integrating grey literature in this review. We also recommend improving the search string and having more flexible filters to include more publications that were not analyzed in this research. Finally, we suggest a comparative analysis between the frameworks and assessment models classified in this research, as well as between the standards and frameworks recognized by the industry.

References


