INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Risks of Robotic Process Automation: A Multivocal Literature Review

António Pedro Brites

Master's in Computer Science and Business Management

Supervisor:
PhD Rúben Filipe Pereira, Assistant Professor,
ISCTE-IUL

Co-Supervisor:
MS José Cascais Brás, Invited Professor,
ISCTE-IUL

November 2022

iscte

TECNOLOGIAS
E ARQUITETURA

Department of Information Sciences and Technologies

Risks of Robotic Process Automation: A Multivocal Literature Review

António Pedro Brites

Master's in Computer Science and Business Management

Supervisor:
PhD Rúben Filipe Pereira, Assistant Professor,
ISCTE-IUL

Co-Supervisor
MS José Cascais Brás, Invited Professor,
ISCTE-IUL

November 2022

"It always seems impossible until it's done."

Nelson Mandela

Acknowledgements

This study was carried out with the support of an exceptional "team", which contributed in a very pertinent way with the sharing of several advices and suggestions. Therefore, I would like to take this opportunity to thank all the people and entities that supported me in one of the most important stages of my academic life.

First of all, I would like to thank unconditionally ISCTE-IUL, in general, from the teachers who instructed me to the remaining colleagues and assistants who accompanied me in this period, in which everyone contributed to a good integration and, fundamentally, to a good and enriching experience.

A special thanks to the Supervisor Professor Rubén Pereira, who is undoubtedly a great example of inspiration in the area to which I refer, having always shown interest, motivation and availability to help.

I also highlight a huge thank you to the Co-Supervisor Professor José Brás, who always trusted in my skills, challenged me and gave me the opportunity to evolve both academically and professionally.

And finally, a huge thank you to my family, especially my parents and sister, who always encouraged me to fight for my ambitions. My girlfriend and best friend, Clésia Varandas, who faced and witnessed by my side this journey with the greatest affection and understanding, tirelessly believing in my abilities. To my long-time friends who gave me strength to continue prioritizing my academic goals.

Resumo

Nos últimos anos, muitas empresas de diferentes setores optaram por apoiar a transformação digital na automação de processos usando RPA. De facto, é possível verificar que as automações têm vindo a revolucionar e beneficiar a força do trabalho humano minimizando as tarefas repetitivas subjetiveis a erros e maximizando a eficiência técnica e operacional das empresas. No entanto, não deixa de ter os seus riscos, uma vez que se fundamenta em robôs desprovidos de qualquer pensamento crítico. Assim, a presente investigação incide num estudo de caso sobre os riscos de RPA, no qual se realizou uma análise profunda, através de um MLR com 107 documentos reunidos e minuciosamente examinados em toda a comunidade, incluindo livros, artigos científicos, relatórios técnicos, conferências, entre outros. Esta investigação contribui com uma lista de um total de 88 riscos organizados, mapeados e agrupados entre 9 categorias. Nesse sentido, este estudo auxiliará futuros investigadores a identificar os riscos de RPA de forma a definirem ações que evitem impactos negativos.

Palavras-Chave: RPA, Robotic Process Automation, Risks, Multivocal Literature Review

Abstract

In recent years, many companies from different sectors have chosen to support digital transformation in process automation using RPA. In fact, it can be seen that automations have been revolutionising and benefiting the human workforce by minimising repetitive tasks subjective to errors and maximising the technical and operational efficiency of companies. However, it is not without its risks, since it is based on robots devoid of any critical thinking. Thus, the present research focuses on a case study on RPA risks, in which an in-depth analysis was conducted through an MLR with 107 documents gathered and thoroughly examined throughout the community, including books, scientific articles, technical reports, conferences, among others. This research contributes a list of a total of 88 risks organized, mapped and grouped among 9 categories. In this sense, this study will assist future researchers to identify RPA risks in order to define actions to avoid negative impacts.

Keywords: RPA, Robotic Process Automation, Risks, Multivocal Literature Review

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AI	–	Artificial Intelligence
CRM	–	Customer Relationship Management
DT	–	Digital Transformation
HR	–	Human Resources
IAM	–	Identity and Access Management
IEEE	–	Institute of Electrical and Electronics Engineers
IS	–	Information System
IT	–	Information Technology
GL	–	Grey Literature
ML	–	Machine Learning
MLR	–	Multivocal Literature Review
PDD	–	Process Design Document
RPA	–	Robotic Process Automation
ROI	–	Return on Investment
SI	–	Sistemas de Informação
SDD	–	Solution Design Document
SLR	–	Systematic Literature Review

Section 1 – Introduction

Today, digital transformation (DT) provides organisations with opportunities to excel through the use of cutting-edge digital technologies [1]. Disruptive technology increasingly plays an important role in all areas of business and is seen as a key driver in changing the way companies create value and gain competitive advantage [2]. With rapid technological changes, companies have been forced to reinvent their business models in order to shorten the time to market for new products and services [3].

Robotic Process Automation (RPA) is a technological innovation that addresses the needs of organisations to keep up with the high pace of technological change [4]. By automating repetitive tasks, allowing employees to make better use of their time on more complex tasks, thus bringing more value to the organisation [5]. With the use of RPA there is a strong impact on a business's operations and competitive positioning on several fronts: economic value, workforce advantages, quality improvements, flexible execution, speed and agility.

According to Gartner, the RPA market reached a 31% growth rate in 2021, meaning it grew well above the 16% average growth rate of the global software market. The latest forecast for the global RPA software market is 18.5% between 2020 and 2022. This year, the market is estimated to be worth $2.4 billion. Continuing double-digit growth is predicted between 2020 and 2022, with a forecast of 17.5% from 2020 to 2023. This will take the global RPA software market to a total of $2.9 billion by 2022 [6].

Although there is much information available on the benefits of using RPA [7] due to the high demand in the business world [4], there are also risks, however, these risks have been few mentioned by authors in the scientific community.

RPA can easily become a risk [8] because it is a tool of consistent and continuous action, any error can become a systematic and widespread problem in the underlying business process and dataset [9]. Therefore, this study aims to identify the risks associated with RPA, creating a framework to develop a risk assessment strategy [10].

To achieve the goal, this study adopted the MLR which aims to incorporate "grey" literature such as blogs, white papers, videos and web pages, which are often produced by professionals outside academic environment, without excluding studies produced by the scientific community, such as scientific papers[11].

This paper is divided into five sections. The first section refers to the Introduction, which highlights the issue under study and the research objective. Then, the second section is devoted to the Background, which presents a theoretical basis on key concepts, namely RPA and associated risks and the same integrated into business continuity. The third section is dedicated to the methodology adopted and developed for this study - Research Methodology. Consequently, the fourth section continues with the Reporting the Review, which answers the defined objective based on the collected information. To summarise, this study ends with a final section, the fifth, where the Conclusion is presented, mentioning the respective theoretical and practical contributions. Furthermore, references are made to the study's limitations, as well as suggestions for future research.

Section 2 – Background

This section is dedicated to Background and seeks to theoretically frame the object of the study. Through key concepts it is possible to clarify critical domains about RPA, potential risks, and how RPA risks impact business continuity. This step of understanding and defining these concepts is very important and will impact the next sections of this research [12].

2.1. Robotic Process Automation

RPA as the name implies is an automation of a robotic process, which is nothing more or less than a software tool capable of automating rule-based processes involving structured data with deterministic results. These tools use programmed robots (software) that follow rules and procedures to perform tasks previously performed by people. The robots interact with the applications in the same way as humans do [13]. Robotic Process Automation is a term that is increasingly being adopted in organizations. Based on a definition and some background, its current use and the value that is returned by its use is discussed. This leads to the identification of the main challenges of current implementation approaches, taking into account the main risks that must be avoided in order for its implementation to be an asset to organizations [12].

In manufacturing environments, robots have been used for a long time [12]. Entire manufacturing lines have been automated using robots to perform manufacturing processes, handle parts, and transport them to other production lines autonomously. With evolution, RPA transfers this process automation approach to the work that employees of IT organizations have been doing [14].

RPA tools, which are commonly called "Bots", are software tools that usually work through a user interface on various computer systems, thus replacing tasks that are normally done by humans. They usually perform simple tasks such as recognizing and reading fields on the screen of some application, modifying content, and exchanging information between different selection fields, all tasks previously programmed by humans following certain rules so that their execution does not incur errors [15].

These Bots perform various steps of different business processes using software tools indicated for each of the processes. Thus, when used frequently, they have a direct impact on the flow of business processes, particularly automated data processing [12]. That said, for simplicity, the definition of RPA can be interpreted through Figure 1.

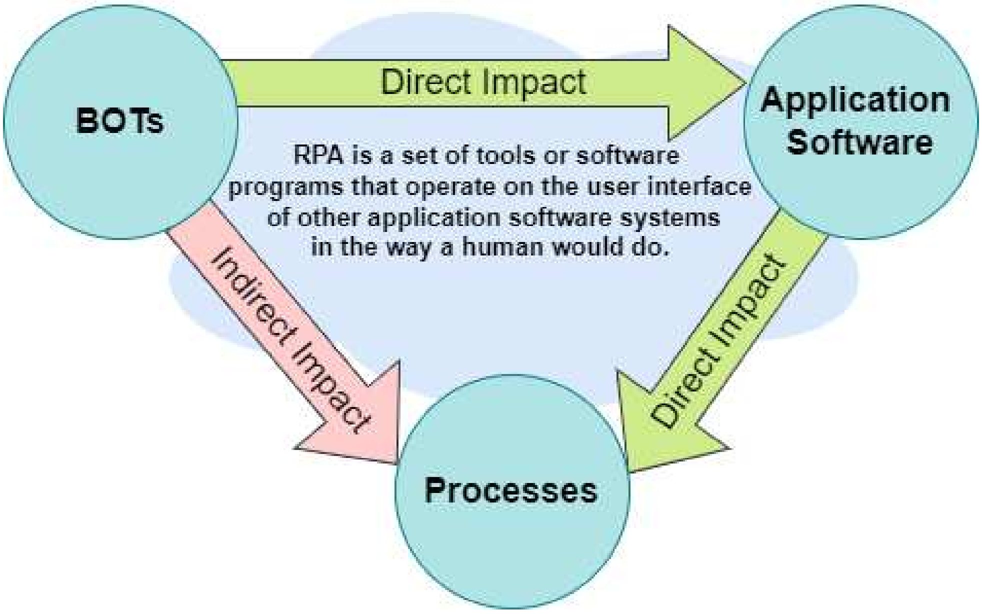
BOTs
Direct Impact
Application Software
RPA is a set of tools or software programs that operate on the user interface of other application software systems in the way a human would do.
Indirect Impact
Direct Impact
Processes

FIGURE 1 - DEFINITION OF ROBOTIC PROCESS AUTOMATION (RPA) [12]

Companies continually seek to lower costs and have increases in efficiency to succeed in an uncertain, turbulent, and competitive environment. Information technology has been, for decades, one of the main strategies adopted to achieve these goals. But process automation can always go further, better articulating different subsystems, or accelerating the connection from analogic to digital [16].

The introduction of processes that seek to improve the quality of the product/service offered, as well as cost retention, are some of the essential paradigms in the eyes of an organization, which can be achieved by creating a connection point between partners/employees and customers [17].

As an example of an RPA process, data linking between applications (E-Commerce) and enterprise software (email address) can be done, and it is possible to instantly associate the customer's name with incoming email, proving to be a value-added measure for the organization. Tasks such as periodic reporting (which includes data analysis), email response generation or automatic date conversion are some of the other real-world examples being performed [18].

So far it is understood that RPA is an approach to process automation across a wide range of different autonomous technologies available on the market. This diversity is justified by the particular characteristics of each automation, allowing a better adaptation to the process in question and the organization's objectives [19].

In this line of thought, RPA integrated into Business Continuity is the transformation of continuous improvement that aims to implement new systems and information technologies in the company, through the automated processes of robotics, in order to improve the quality of services provided, driving an improvement in the effectiveness of response, the efficiency of its processes and a subsequent rationalization of operating costs [19]. Thus, through the integration of RPA it will be possible to achieve better levels of efficiency and productivity at the operational level. With the integration of these automatisms in the various organizational processes, institutions will be able to perform routine operations in an automated way, even outside working hours, thus reducing operating costs associated with the execution of these processes and the operational risk associated with manual execution errors [20].

On the other hand, there are still challenges to its proper implementation in organizations, as well as a priori conditions established to enable its efficient operation [21]. In order to optimize the efficiency of RPA, it is necessary for companies to establish appropriate processes for its use, which means seeking to align management criteria and objectives with the technology that is to be implemented [21]. Otherwise, any RPA failures that occur during or after implementation may negatively impact your business continuity and are considered potential RPA risks. A risk can be explained as an uncertain event that negatively affects the operation or cycle of the RPA implementation. One of the weaknesses pointed out to RPA is the need to have properly established rules, since software robots are devoid of any critical thinking. From this perspective, normalizing the process before using these robots is crucial, since the more normalized the method, the less susceptible to exceptional errors [22].

Furthermore, studies indicate that frequent use of processes that require the human user to complete a multi-step task is more susceptible to errors. Thus, the use of a robot would then be especially advantageous in this type of situation [23].

As discussed in the subsections above, RPA emerges as a business process solution based on automation software, mainly targeting repetitive tasks that consume a lot of processing time. In fact, some of the main areas of automation implementation in businesses concern accounting functions (accounts payable and receivable, fixed assets), travel booking, expenses, and human resource administration. In addition, human management control in processing can limit the autonomy of automation effectiveness, due to the problem of the robot's lack of critical intuition

[12]. Due to these reasons, software robot-supported automation is mainly applied to routine tasks and then serves as a bridge between human work and full business process automation, as shown in Figure 2 [24].

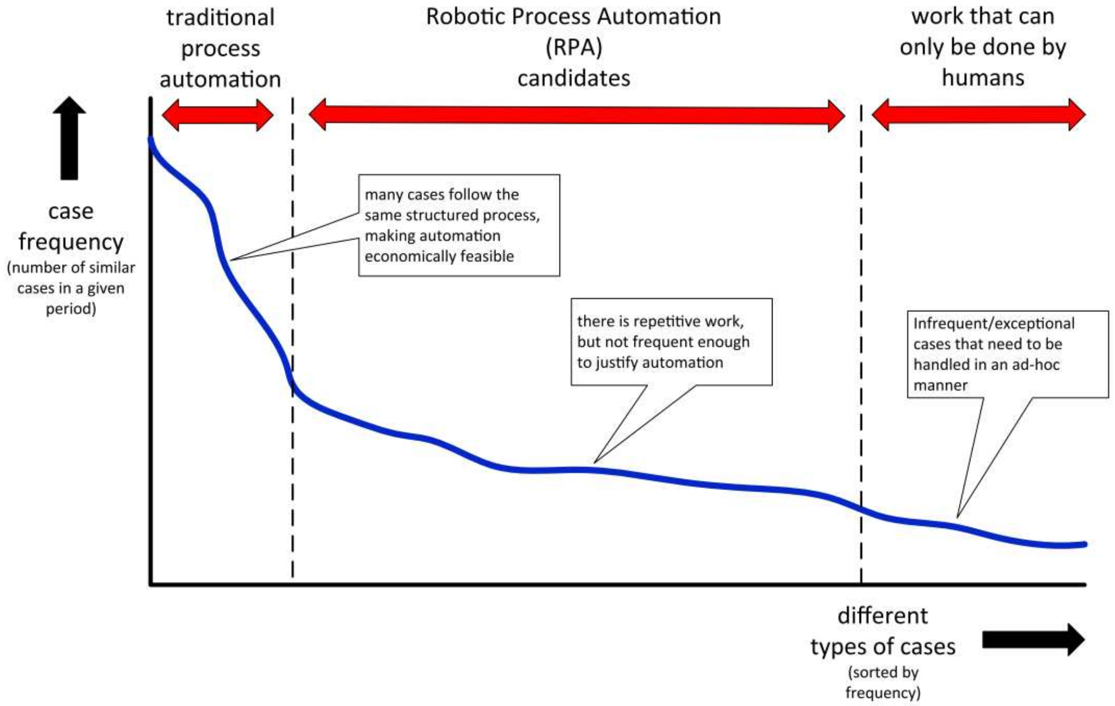

FIGURE 2 - POSITIONING RPA [24]

To maximize their utility, providing an intuitive interface in the development environment will promote ease of use and implementation. Thus, companies can build software robots by rearranging a sequence of configurable modules that allow them to control operator flow to create a choreography according to business needs [23].

Adding to the above, ease of use continues to be mirrored in the creation of software robots: where for a user it is sufficient to delete, add, move, or reconfigure elements to achieve that goal. Since there is no need to extensively introduce or reconfigure new information systems and since business processes generate data in a decentralized manner with different structures, software robots also provide an integration function [24].

This function allows them to control/access applications or services automatically and to interconnect different data silos, thus allowing robots to control information flow operators [25].

Given the above, not all processes will be as complex as described. As an example, an RPA process could be related to automating simple tasks. A robot could open a new Microsoft

Excel tab, navigate to a specific sheet and change values in specific cells, save the changed sheet and close the application [26]. As can be seen, the proliferation of technology has brought profound changes in a wide variety of industries, with the business context, in particular, being the most impactful [18].

This topic concludes on the belief that RPA, proves especially useful within management, articulating the passage of data between different applications or automating other tasks reducing human intervention. Software robots are beginning to be used to replace human actors in certain tasks, seeking to increase the efficiency of business processes, thus benefiting organizations [17].

However, since these automated processes highlight some risks, this study aims to conduct a survey of the risks in order to identify them, contributing in the scientific community so that companies and future experts can drive actions that mitigate potential threats in business continuity.

This section is dedicated to Background and seeks to theoretically frame the objective of study. Through key concepts it is possible to clarify critical domains about the RPA, and potential risks.

Section 3 – Research Methodology

In order to conduct this work we used an Multivocal Literature Review (MLR) [27], this is a systematic review method that also covers Grey Literature (GLR) like the articles published in blogs, web pages, White Papers and videos, which are constantly produced by professionals linked to the IT area outside the academic context. Being so, MLR's have a relevant importance for the research expansion, because otherwise this literature would not be considered valid for the study of this research (for being of "grey" nature), as we may observe in Figure 3 [28].

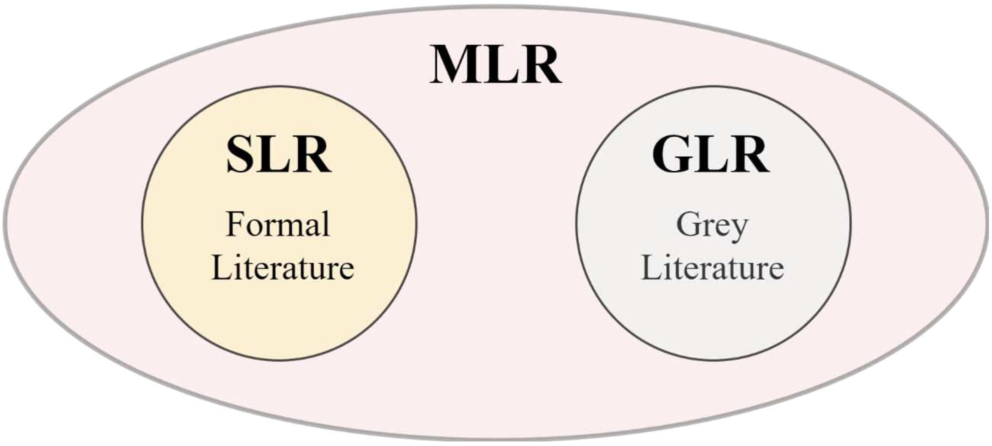

FIGURE 3 - RELATION AMONG SLR, GLR AND MLR [28]

Due to the fast evolution of IT, several researchers have already realized that including the GLR brings benefits to the study review, because it is a way to add value and knowledge without compromising the viability of the information. Some examples of successful studies (linked to the IT area) which also used MLR already exist [5][29][30]. This way we were able to confirm the practical usefulness of this method and apply it in this research, contributing to the diversity of different sources of knowledge that are currently available in various forms, with different perspectives and objectives [31].

The research of this MLR aims to discover which are the major risks of RPA implementation described by the various professionals in the field, and to be able to detail them thoroughly by finding out if there is a consensus on the best way to avoid these risks during its implementation. For this, we have the need to expand this study beyond the limits of scientific knowledge, thus, MLR gives us this opportunity, and manages at the same time to maintain a rigorous quality in the process of analysis of this literature [31].

In Table 1, we can observe the separation of the different sources of the "white" and "grey" literature, and the set of the two forms of the MLR. Note that, for greater credibility of the data, articles extracted from social networks, tweets and emails were excluded from the literature that corresponds to ideas, concepts and thoughts [27].

TABLE 1 - SPECTRUM OF THE "WHITE", "GREY" AND EXCLUDED LITERATURE [27]

"White" literature	"Grey" literature	Excluded literature
Published journal papers	Blogs	Ideas
Conference proceedings	Technical reports	Concepts
Books	Audio-Video (AV) media	Thoughts
	Lectures	
	Data sets	
	Preprints	
	e-Prints	

There are numerous guidelines for conducting an SLR study. However, there are several phases of MLR that do not coincide with traditional SLRs. One of these is the process of assessing the quality of the source of information and its investigation. Therefore, we will partially use the SLR guidelines to carry out this MLR. We can observe by Figure 4, the structure of the guidelines for this MLR, where it shows the planning, conducting and reporting exactly as it was proposed by Garousi et al [27].

With the implementation of this model, it is expected that the grey literature will provide us with important knowledge about the risks of implementing the RPA, not disregarding that this will bring new challenges when including such literature, as the knowledge provided is often based on the experience and opinion of those working in the field. For this reason, in this research, I will use systematic guidelines to perform MLR [28] and thus achieve a consistent and concise data collection similar to what is done in an SLR, applying to it the inclusion and exclusion criteria in the results obtained through the world's most well-known search engine called Google.

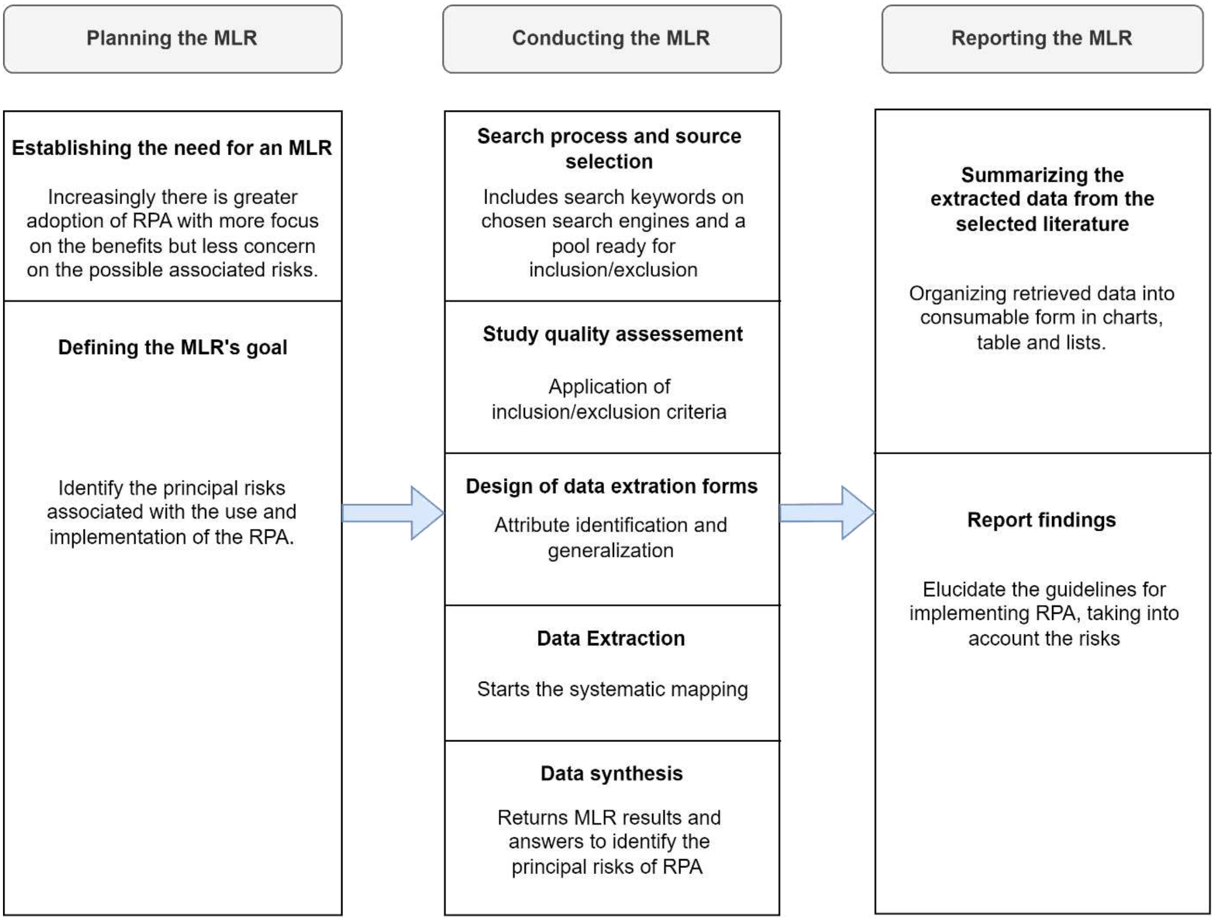
Planning the MLR
Conducting the MLR
Reporting the MLR
Establishing the need for an MLR
Increasingly there is greater adoption of RPA with more focus on the benefits but less concern on the possible associated risks.
Defining the MLR's goal
Identify the principal risks associated with the use and implementation of the RPA.
Search process and source selection
Includes search keywords on chosen search engines and a pool ready for inclusion/exclusion
Study quality assessement
Application of inclusion/exclusion criteria
Design of data extration forms
Attribute identification and generalization
Data Extraction
Starts the systematic mapping
Data synthesis
Returns MLR results and answers to identify the principal risks of RPA
Summarizing the extracted data from the selected literature
Organizing retrieved data into consumable form in charts, table and lists.
Report findings
Elucidate the guidelines for implementing RPA, taking into account the risks

FIGURE 4 - MULTIVOCAL LITERATURE REVIEW (MLR) STEPS ADOPTED IN THIS RESEARCH [27]

3.1. Planning the Review

This section represents the first phase of the MLR implementation. It starts with the motivation that led this subject to be studied, then what are its objectives, and what are the research questions we propose to answer with this research.

3.1.1. Motivation

As can been seen at Figure 5 that it was from 2016 that RPA started to have some impact on the searches made by users on the world's largest search engine, google.

Its trend is clearly increasing, which can be a positive sign that organizations are increasingly investing in this theme. Being a recent topic in the scientific community it becomes an extra motivation to explore this subject.

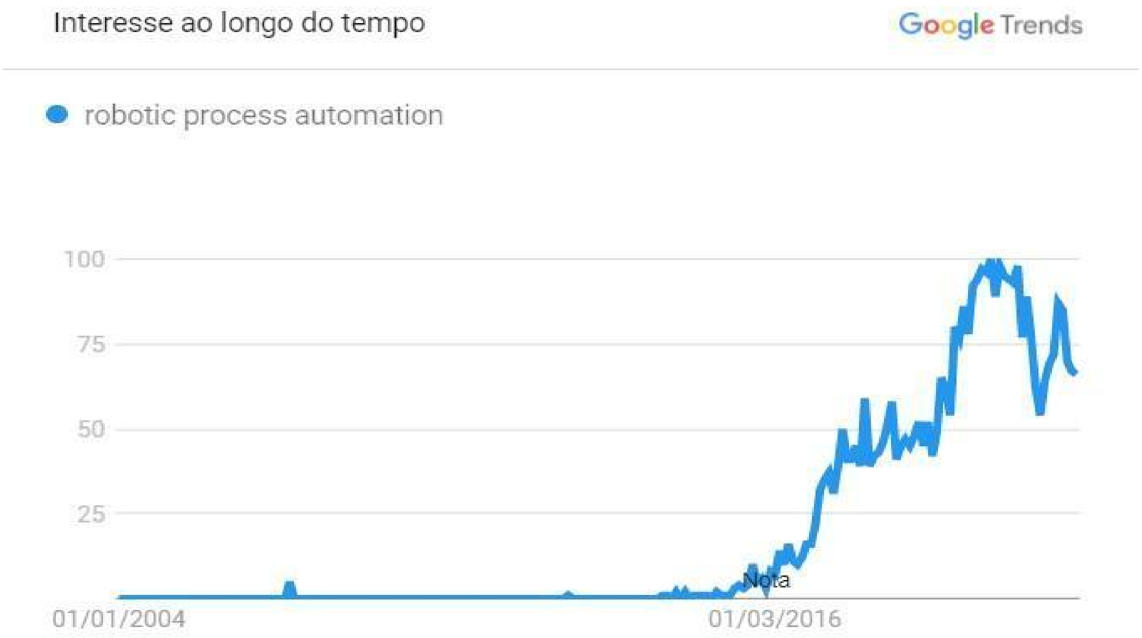

FIGURE 5- INTEREST IN RPA OVER TIME (GOOGLE TRENDS)

3.1.2. Establishing the need for an MLR

After brief research on the topic, it was found that organisations tend to adopt competitive strategies in the IT market. Since RPA is a new technology in increasing demand, companies do not want to be left behind by their competitors. Thus, the first requirement that companies sought to know was what kind of benefits and value RPA can bring to their organisations.

Without further hesitation, to keep up with the rapidly changing market, organisations started implementing it and as a consequence, there is increasingly adoption of RPA with more focus on the benefits but less concern about the possible risks associated with it.

Thus, it became interesting to focus this study on the risks associated with RPA to alert that in beyond the benefits there are also risks and it is a way to complement all the existing information about the risks of RPA.

3.1.3. Review Protocol

To obtain answers for this study it was necessary to search and find other relevant studies through keywords that formed a search string. In Figure 6, it is possible to observe the steps that were followed until arriving at the basis of the final document. In an initial phase, the keywords that gave rise to the search string were chosen and used in the selected databases.

Keywords:

- Robotic Process Automation / Intelligent Process Automation / Risks

Search String:

- (Robotic Process Automation OR Intelligent Process Automation) AND Risks)

Datasets:

➢ IEEE Xplore	(https://ieeexplore.ieee.org)
➢ ACM DL	(https://dl.acm.org)
➢ Scopus	(https://scopus.com)
➢ Web of Science	(https://apps.webofknowledge.com)
➢ EBSCO	(https://search.ebscohost.com)
➢ Springer	(https://springer.com)
➢ Google Scholar	(https://scholar.google.com)
➢ Google Search	(https://google.com)

After defining the search string and the datasets that are to be used for searching, data retrieval was started. For the scientific search part, the search string was used in all the indicated databases except "Google Search". In obtaining the grey literature, to facilitate the massive search of this topic, a bit of code was developed that was adapted from article [32] which can be seen in appendix A (Python code to get the Google Search results). This way, the search is done massively and transferred directly to a CSV file [33]. With this search method, it was ensured that the results are not specific to a particular user, as Google targets searches according to usage history and search preferences. In sum, clean results were obtained that are easily consumed and used in the use of grey literature.

After the search, filters were applied to all databases used. Once the reference of the documents was filtered, a manual analysis was performed after obtaining the data, where it was checked if the document was complete and accessible, thus avoiding incomplete documents and also discrepancies between the representation of the results and the files actually obtained. Finally, the exclusion and inclusion criteria were applied, which can be seen in Table 2.

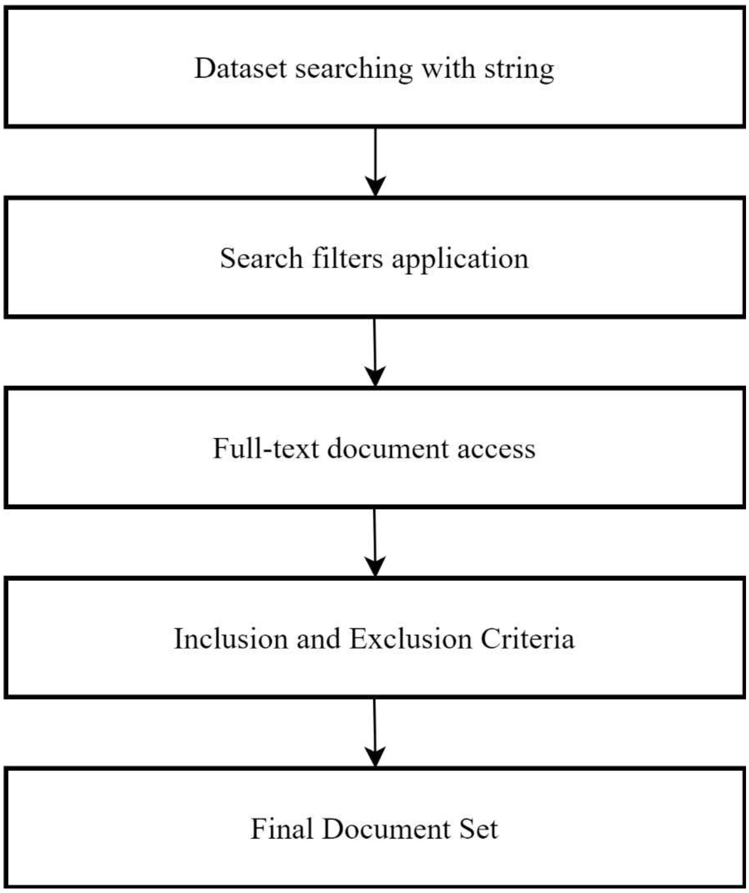
Dataset searching with string
Search filters application
Full-text document access
Inclusion and Exclusion Criteria
Final Document Set

Figure 6 - Review protocol performed in this research

The exclusion and inclusion criteria used in this work are represented in Table 2, and aim to eliminate, mainly from the grey literature, articles that are not related to the theme, that do not have a defined date and author and that are not advertisements or posts. In this way, the extraction of data from the grey literature has more quality and its information is quite specific and more credible.

Table 2 - Inclusion and Exclusion criteria applied in this research

Inclusion Criteria	Exclusion Criteria
Written in English	Unidentified author
Mention RPA or IPA and risks	No publication date
	Advertisement or Job Post

3.1.4. Defining the MLR goal

As seen in Figure 4, the MLR planning phase is subdivided into two phases, and after completion of the first phase where the need for the MLR was established in relation to the topic, a main goal was defined which aims to identify the principal risks associated with the use and implementation of the RPA.

3.2. Conducting the review

After planning the MLR, comes the conducting phase, where it has been divided into five distinct phases. In the first phase of the process the GL search is usually done through the use of search strings. Next there is source selection, which usually includes selection criteria and the possibility of performing filtering. Then a source quality assessment study is performed to determine the veracity of the knowledge sources and have the ability to identify them as valid.

After the evaluation is complete, comes the phase of data extraction in a systematic way, with logical procedures and with the possibility of extracting the data automatically. Finally, a synthesis of data is performed with quantitative and qualitative techniques.

3.2.1. Selection of studies

This section presents how the filtering of the articles was done and what the final result of the documents is, including figures and tables representing the extraction process. All filters applied are cumulative.

The first filtering consists of searching for exact matches, thus looking for the exact set of keywords, without the words being searched individually and separately. At this stage, a total of 671 articles were retained in all databases.

In the second filtering, a search cut-off date was applied, where only articles dated 2016 or later were retained, thus avoiding articles that are not directly related to the intended subject, because as can be see in Figure 5, 2016 was the date when the subject started to have some relevance on the Internet and, consequently, in the scientific community. At this stage, 632 articles remained.

After applying the search deadline, the search for keywords with exact matches only in the abstract was started, thus significantly reducing the dataset, and obtaining documents very close to the intended subject, which represents a total of 260 articles. Note that it was not possible to apply this filter in three databases, Springer, Google Scholar, and Google Search.

To ensure the reliability of the documents, a manual review was performed in this filtering phase, where it was checked if it was possible to access the document without any restriction and also if the document was complete and without missing parts, as happened in the links obtained in Google Search, which were sometimes parts of books or articles without access permissions. Thus, at this stage, 200 articles are filtered.

The next filtering process was done through the Mendeley software, where all the documents up to that point were loaded, and using a feature of the program, all duplicate documents were eliminated, leaving 189 unique articles.

Finally, the inclusion and exclusion criteria were applied, where the criteria were previously defined as shown in Table 2. This filter was applied mainly for the search in the Google Search database, because in this way it was guaranteed that only articles written in English, which mentioned the intended topic, were extracted, and articles that had no author, thoughts, or advertisements and posts defined were excluded. After applying this last filter, 107 articles directly related to this study remained.

As can be seen in Figure 7 the whole process in an illustrative and easy to understand way, where all the databases used, the filters applied, and the final result of this process are represented.

3.2.2. Data Extraction Analysis

In this section an analysis of the selection of the final set of publications was performed, where it is explicitly represented which and how many documents were extracted from each database after applying all filtering criteria. It is possible to distinguish how many articles represent the "grey" literature, which are represented by web pages and tech reports and how many belong to the "white" literature, which are the traditional scientific articles and books.

Table 3 shows the number of articles extracted from each database, showing all the results after applying each single filter. All the filtering criteria were very important to restrict the information in order to obtain only relevant articles for this study. Table 3 shows that before applying any filter, there was a total of 112,316 articles searched by only keywords.

After the first filter, there is an abrupt reduction in the results, because by searching the keywords with exact matches all articles that refer to isolated keywords such as "Robotic", "Process", "Automation", among others were excluded. This way, it forces the search result to contain all keywords in a single meaning, obtaining only results that contain the complete keyword "Robotic Process Automation".

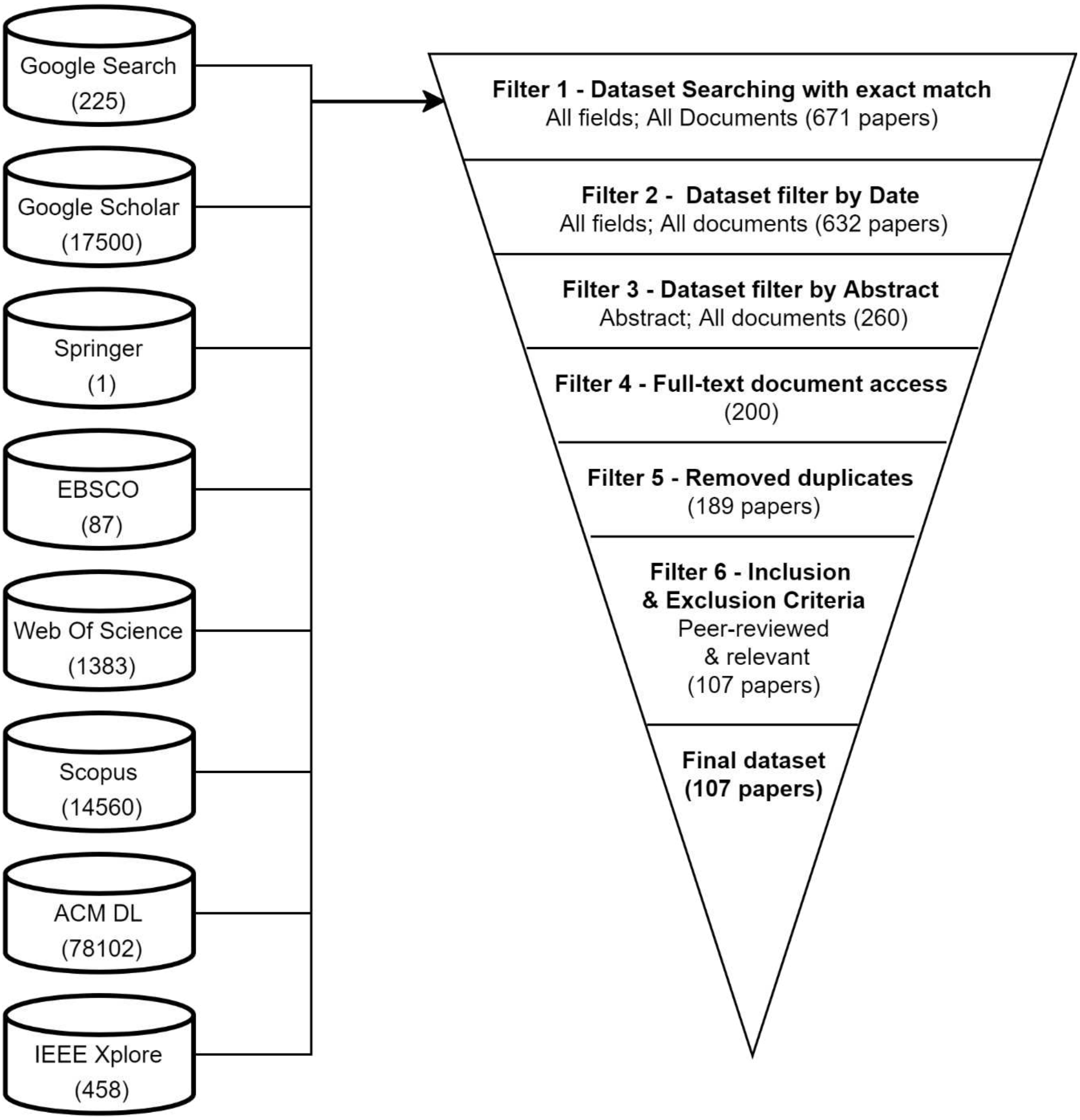
Google Search
(225)
Google Scholar
(17500)
Springer
(1)
EBSCO
(87)
Web Of Science
(1383)
Scopus
(14560)
ACM DL
(78102)
IEEE Xplore
(458)
Filter 1 - Dataset Searching with exact match
All fields; All Documents (671 papers)
Filter 2 - Dataset filter by Date
All fields; All documents (632 papers)
Filter 3 - Dataset filter by Abstract
Abstract; All documents (260)
Filter 4 - Full-text document access
(200)
Filter 5 - Removed duplicates
(189 papers)
Filter 6 - Inclusion & Exclusion Criteria
Peer-reviewed & relevant
(107 papers)
Final dataset
(107 papers)

FIGURE 7 - FOLLOWED MULTIVOCAL LITERATURE REVIEW PROCESS (ADAPTED) [27]

Another filter that also had a strong impact on the tapering of the articles obtained, was the F3 (Query Abstract with exact match and date ≥2016) that forces the keywords to be referenced in the abstract, being ensured that the information that is extracted from these documents has a strong possibility to meet the expectations and satisfy the needs of this study.

Finally, and after all the filters applied, 107 carefully selected articles remained, all of which contain useful and relevant information to be analysed and studied to contribute positively to the report of this study.

Search String:

- (Robotic Process Automation OR Intelligent Process Automation) AND Risks

Table 3 - Filters used in the MLR protocol

Base de Dados	Initial	F1	F2	F3	F4	F5	F6
IEEE Xplore	458	4	4	3	3	3	1
ACM DL	78102	30	22	1	1	1	1
Scopus	14560	292	292	21	13	13	6
Web of Science	1383	75	47	3	3	3	1
EBSCO	87	77	77	42	14	8	2
Springer	1	1	1	1	1	1	1
Google Scholar	17500	11	11	11	11	11	11
Google Search	225	181	178	178	154	149	84
Total	**112316**	**671**	**632**	**260**	**200**	**189**	**107**

**Underlined means the number came transferred from the previous filtering due to the impossibility of executing F3*

Initial: Search keywords without filtering
F1: Query All fields with exact match
F2: Query All fields with exact match and date ≥ 2016
F3: Query Abstract with exact match and date ≥ 2016
F4: Full-text Document access
F5: Remove duplicates
F6: Inclusion and Exclusion criteria

To be graphically visible, Figure 8 was drawn, which shows in a simple and succinct way how many articles were extracted from each database. It is easily observed that the largest "ball" corresponds to Google Search database with 78.50% of the matches. The remaining databases add up to 21.50% of the remaining matches, as can be confirmed in Figure 8.

Observing the figure, it is possible to conclude that there is a strong discrepancy of mentions between the traditional databases with scientific articles and articles posted by professionals in the area outside the academic world, "grey" literature. Adopting the MLR for this study, will be an added value to contribute positively to the transfers of relevant information to the academic world, obtained from both literatures combined.

It should be noted that, although Google Search represents almost all the grey literature, important scientific articles were also found and extracted through this search.

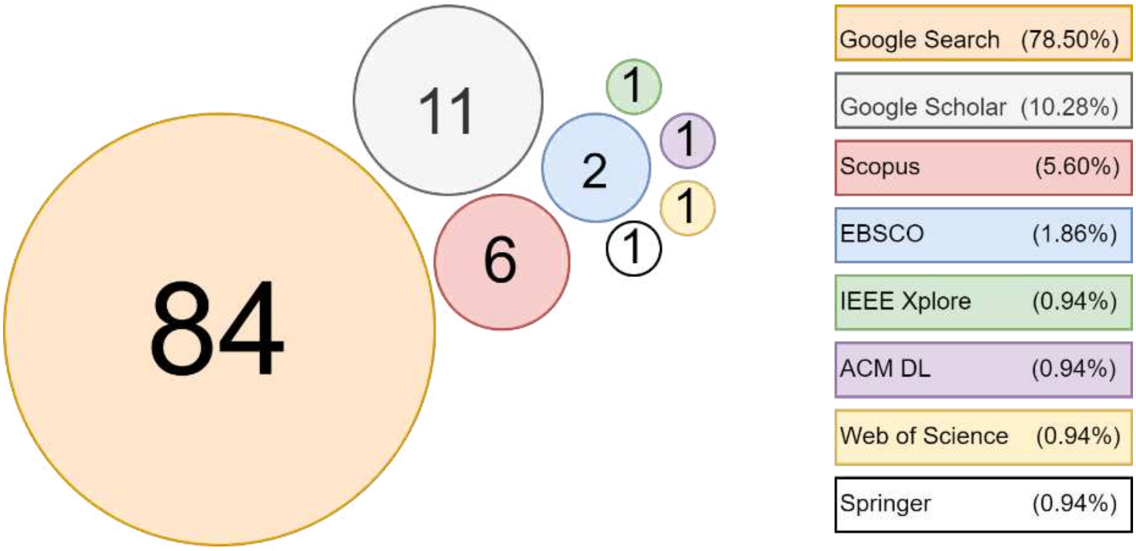

FIGURE 8 - DISTRIBUTION OF THE FINAL SET OF DOCUMENTS PER DATABASE

3.2.3. Grey and white literature number of contributions

To complete this analysis, a graph was prepared, represented in Figure 9, where the main observation is the number of articles that represent the grey literature, adding a total of 78 articles obtained through webpages and techreports, representing 73.90% in a total of 107 articles.

All the others, represent the scientific literature, through scientific articles and books, adding up to a total of 27.1%, which makes a total of 29 articles.

In summary, it is easily observed that the "grey" literature has a greater impact on the performance of this study, due to the scarcity of content on this subject in the scientific community. Thus, the MLR is quite powerful since it can combine both literatures in order to obtain reliable and trustworthy information.

3.2.4. Distribution of publications over the years

Given the exponential increase in interest and volume of work around the areas of RPA, it is important to detail and analyse this same differentiated and distributed growth over recent years as shown in Table 4 from where Figure 10 was generated.

TABLE 4 - GREY AND WHITE NUMBER OF CONTRIBUTIONS OVER THE YEARS

Publications	2016	2017	2018	2019	2020	2021	Total
Techreport	1	3	9	2	4	3	**22**
Webpage	1	3	5	11	16	20	**56**
Article	0	2	3	8	9	5	**27**
Book	0	1	0	0	1	0	**2**
Total	**2**	**9**	**17**	**21**	**30**	**28**	**107**

As mentioned in previous sections, the first extracted publications started to appear in 2016 through a Techreport [34] and a Webpage [35].

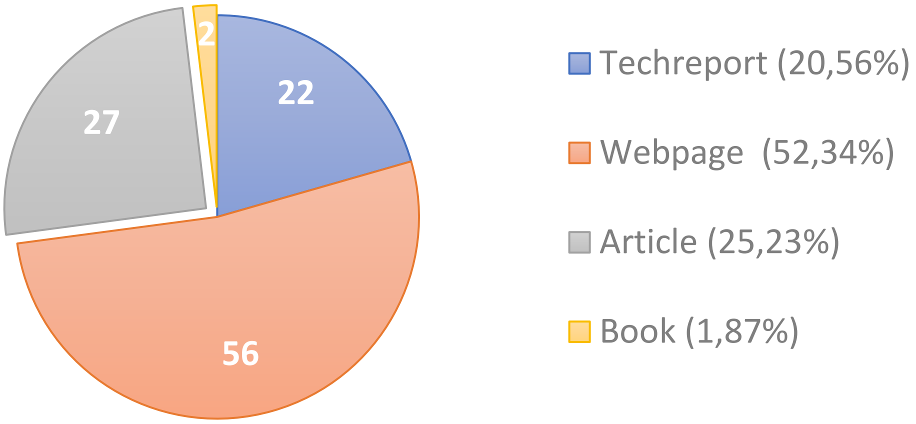

FIGURE 9 - GREY AND WHITE NUMBER OF CONTRIBUTIONS

In 2017, there is a continued growth of Techreports and Webpages. In addition, it was in the same year that other publications began to appear in 2 articles [13][36] and a book [25].

The following year 2018 saw a significant increase and interest of related publications in the grey literature between Webpages and Techreports but with a higher focus on Techreports, a consequence of the emerging integration of this technology of companies and in corporate activities. Furthermore, this increase indicates that professional publications have evolved much faster than scientific research.

Thereafter, between the year 2019 and 2020 there is a gradual increase in total publications, and in 2021 the numbers of publications slowed down slightly from the growth observed. However, it is important to detail that in 2019, unlike 2018, the publications related to grey literature, Web Pages had a higher incidence. In addition, it was the same year in which scientific literature began to gain space in the scientific community.

In 2020, within the defined period under analysis - from 2016 to 2021 - was the year in which the largest number of publications was observed, resulting in 4 Techreports, 16 Webpages, 9 articles and 1 book, making a total of 30 publications. Curiously, despite a brief reduction in publications in 2021, Webpages continued to grow standing out over time, presenting a greater number compared to the other types of publications over the years, with total evidence of 20 references in 2021.

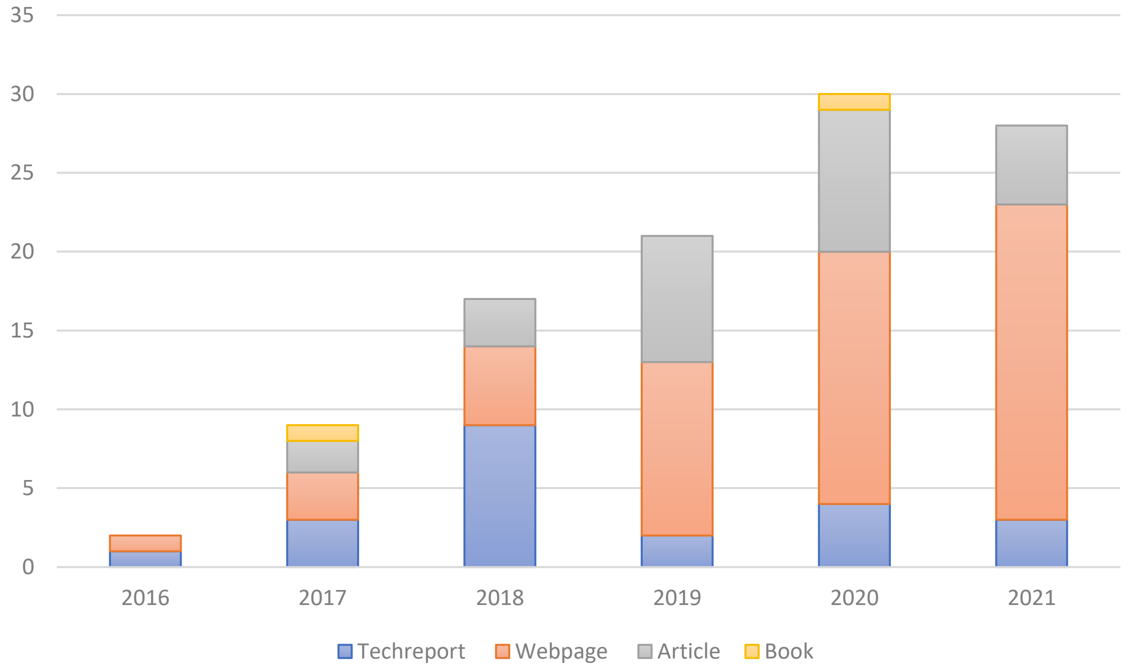

FIGURE 10 - DISTRIBUTION OF PUBLICATIONS PER TYPE OVER THE YEARS

In summary, in general the result of the publications has been more referenced in grey literature than in academic literature proving that this subject is a recent study with few precedents in the scientific community.

Section 4 – Reporting the review

The reporting phase of an MLR includes: summarizing the data extracted from the selected literature and also its conclusions, which is similar to that of SLR [11].

4.1. Results Analysis

The objective of this research is to identify the principal risks associated with the use and implementation of RPA, and to facilitate the framing of all these risks, the main risk groups were created to give us a more peripheral vision of the positioning of each risk. From here it was also possible to understand which ones have the greatest impact based on existing extraction from the grey and academic literature. Thus, the following subtopics aim to respond in detail to the goal defined in this research.

4.2. Main group risks

To implement RPA, it is necessary to know how to face the risks that it warns about and how to frame them in the right way. And according to the research done for this study, several authors have framed the risks into different major groups [25][37][38][39]. Groups where in general there is a consensus that the main risks can be categorized. A first prototype of risk groups was formed, starting with Strategy Risks, Sourcing Risks, Tool Selection Risks, Stakeholder buy-in Risks, Launch/project Risks, Operational/execution Risks, Change Management Risks and Maturity Risks, which represents the eight groups mentioned.

Next, it was verified that there was a great concern with Security Risks [40][41][42], which originated another large group of risks associated with the security of RPA use and implementation, the Security Risks group.

Finally, and to finish, making a general evaluation of all the risks that the authors mention, another large group was formed, the cross-cutting risks, and this gave rise to the summary in Figure 11.

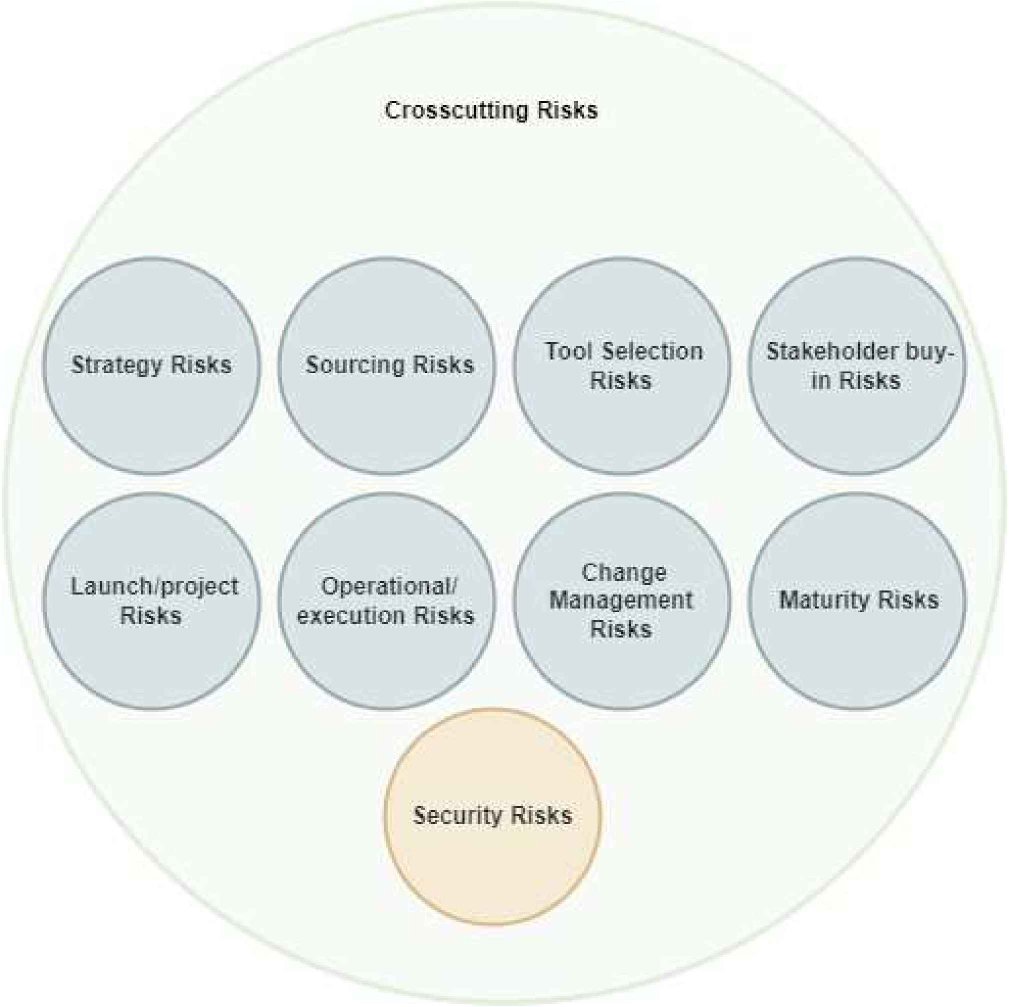

FIGURE 11 - MAIN GROUP OF RPA RISKS

4.2.1. Strategy Risks

RPA strategy risks. The biggest strategic risk involved is thinking that RPA is a tactical tool to cut costs on specific tasks within one department of an organisation. A misinterpretation of the use of RPA can bring significant losses of value after its implementation [23][38][43].

Where organisations have overlooked this risk, one of the reasons this may have happened is because the RPA tool is under-resourced, however the worst mistake in this section is to look at automation as a way of shortening work rather than changing the way work is done [22][44][45].

4.2.2. Sourcing Risks

RPA users run the risk of leaving value unused or incurring excessive costs by choosing the wrong sourcing model [9]. Some organisations tried their best to develop and execute robotic automation operations but lacked the technical skills to do so [46].

Organisations took on the support of their RPA suppliers, but these too were too busy responding to the increasing needs of the rapid demand for automation from other organisations [39][47]. Choosing the wrong advisors, thinking they were already far advanced in their research on this topic, is a problem that still occurs today. Sometimes organisations sold their software without having it thoroughly tested [37][38][48].

4.2.3. Tool Selection Risks

Due to the hype and confusion in the market, customers buying RPA ran the risk of choosing the wrong, too many, or even poorly developed tools [37][38].

As this market is very new, many companies sold their product as an RPA while others sold a product claiming to be just a form of automation [46]. Anyone who purchases an RPA tool should consider the reliability of the advertising of that tool. "RPA washing", refers to the phenomenon of companies spending more resources on advertising and marketing, which claim to have new service automation capabilities, however these capabilities they acclaim do not correspond to reality [39][46][48].

4.2.4. Stakeholder buy-in Risks

RPA initiatives require buy-in from IT stakeholders, employees, and customers, both internal and external to the organisation. Some organisations were sceptical of IT staff trying to implement automation in their departments, as their management felt that it was not something new and innovative and that it threatened the stability and security of the system they had in place [25].

There are situations where business users blame the RPA for incorrectly performing the tasks that were imposed on it, but they did not realise that the RPA was only performing the tasks it was programmed to do [49]. On the other hand, there are situations in which it is so effective that nobody notices that its execution is being extremely important in the functioning of the organisation [20]. Note that users of RPA are an integral part of successful delivery and need monitoring as the software can stop or fail to run.

4.2.5. Launch/project Risks

Organisations must mitigate various risks to prevent the initial risks of technical, financial, and political failure. Some companies choose only large projects because they think it will generate more financial results, but the rollout fails because processes are constantly changing and require too much exception handling [37][46][50].

Failure also results from unrealistic project estimates particularly for business cases that were too aggressively targeting immediate savings from process automation. Organisations that are forced to meet tight deadlines tend to want to use automation excessively and try to create or acquire a tool to help achieve the goals set by the organisation's management, which turns out to be a very expensive path and the results are usually not achieved [51].

4.2.6. Operational/execution Risks

Operational risks occur when robots are transferred to development in operations without proper verification or a well-defined execution mode [25]. Some organisations do not define well the execution roles, and after its launch each employee uses the RPA according to their understanding [37][46]. This creates many doubts and discrepancies in its use. The boundaries of responsibilities are blurred and end up generating an additional problem to the organisation instead of solving and optimising situations.

Another operational risk is the lack of testing before going productive and sometimes the problem was that the RPA did not have the capacity to be executed in large volumes, which ultimately resulted in not using the development [46]. This clearly adds to the expense of operational execution and maintenance that is not used optimally.

4.2.7. Change Management Risks

These risks are strongly linked to strategy, stakeholder buy-in launch as well as operational risks [46]. Poor communication of strategic intent, not actively seeking stakeholder buy-in and not managing operational dynamics together are cumulative risks of managing multiple changes [39].

Changes in management capabilities are required to keep strategy, processes, technology, and people aligned throughout the RPA implementation process and need to be funded [52]. As for human resources they must be continuously trained and motivated to execute future work, otherwise resources will struggle to build a mature capability to deliver business benefits [46].

4.2.8. Maturity Risks

When previously identified risks are mitigated, companies often experience the value gained from their first implementations. The goal is to expand these implementations in a sustainable way, however this expansion can be impeded due to several risks. Without good coordination, efforts in implementing RPA can be duplicated and there is underutilization of its use [46].

After a successful implementation, organizations tend to focus only on RPA and forget about the bigger picture of preparing for further automation advances [38]. As a result, new developments are constrained by skills shortages and slow down the learning dynamics of automation [46][48].

4.2.9. Security Risks

The high demand for RPA has led to security issues being raised. Robots with RPA can handle sensitive data, moving it through systems from one process to another. If the data is not protected, it can be exposed and cost organizations millions of dollars. [40].

Organizations must put in place data governance, management, and security frameworks to protect data that is processed by Data Process Automation BOTS. These frameworks should be integrated as part of a broader cyber security strategy [53].

4.2.10. Crosscutting Risks

Initially the risks were identified and mapped into major groups, but after a thorough analysis of the conceptualised model it was found that some of the risks could also be considered in other major groups. From this conclusion these risks were considered cross-cutting risks. These categories of cross-cutting risks are detailed in the next section dedicated to the Framework of this research.

4.3. Risks of RPA

Throughout this research, it has been verified that there are several specialists who agree that the adoption of RPA radically transforms companies' operations, combining an improvement in service quality with a reduction in costs and processing times.

On the other hand, there are also negative points to the implementation of RPA. In this line of thought, the objective of this study aims to determine what the risks of RPA are. In fact, through in-depth research it was possible to extract the theoretical framework of the risks associated with RPA and define the respective major groups related to its implementation. In the following subsections it is possible to understand in more detail all this analysis carried out on the major risk groups.

Through the analysis and conceptualization of the major risk groups it was possible to identify 88 risks, in detail in Table 5 (appendix B). Before discussing each risk, it is important to mention that the list presented is supported by the literature review of 107 publications. Thus, this list includes the name of each risk and the number of publications in which they were mentioned, as can be seen in Table 6 (appendix C).

ST01 – Misunderstood or missed value is mentioned in 4 publications and means that the value offered by the RPA implementation is missing or not understood [38]. The strategy applied is not considering the three main values, shareholder value, customer value and employee value, which consequently does not bring value to the organization [25].

ST02 - Lack of strategic intent, is mentioned in 11 publications and can mean a miscalculation of which parts of the process are most suitable for unassisted versus assisted RPA [47]. Organizations can also fall behind when they do not develop a digital transformation strategy that takes into account a broader view of productivity and cost [54]. Organizations often enter robotics prematurely, without doing careful planning and evaluation first. This can lead to costly missteps and waste of time. There are many things you can do to prevent this. One example is conducting a feasibility assessment in order to correctly identify the core process on which you should focus [55].

ST03 - Absence of endpoint design, is mentioned in 5 publications and is when RPA is treated as a series of automations of manual work, not as an end-to-end continuous improvement program [47]. It is also often the case that you want to skip steps in implementing RPA, but this will lead to later calibration errors. It is also important to mention that nearly half of all RPA systems fail when first implemented, so it may require more resources than initially thought [52].

ST04 – Isolated/one off goals, is mentioned in 7 publications and is when RPA implementation focused only on reducing work [43] or for example when organizations with Automation Islands the different lines of business each have their own independent automation that is vulnerable to bot stops and RPA downtime. Different practices in automation designing as well as poor knowledge sharing and mistakes lead to high costs and lower quality over the long term. [22].

ST05 – Under-resourcing your RPA projects, is mentioned in 3 publications and is a risk that can be a consequence of the risks mentioned above, the lack of ability to define objectives can force RPA projects to be outsourced not for the best reasons [25].

ST06 – Poor strategic reputation, is mentioned in 2 publications and means that the application of a bad implementation strategy creates a bad reputation both internally within the organization and externally for RPA service providers [25].

ST07 – Fails to develop a solid business case for RPA, is mentioned in 2 publications and may occur when implementation planning is postponed until after the pilot phase [47] this can be due to either insufficient definition of business rules or by ordering the wrong parts of the system [12].

ST08 – General lack of oversight of risk, is mentioned in 4 publications and it can affect the strategy by unexpected problems that are not being monitored [56].

ST09 – get and secure development and management of bots, is mentioned in 3 publications. Bots need management, maintenance, and security. Implementing many bots to automate processes often requires different types of technology and integration, which encompasses a lot of additional IT overhead. By adding another layer of architectural complexity, IT needs to spend time to ensure that its RPA implementation is solid and works as it should [57].

ST10 – Poor governance of RPA, is mentioned in 7 publications. To better explain this risk, let us look at it as an example: Your company has been using RPA for some time and you decided to assess the IT risks through an independent analysis. A report was prepared by a well-known consulting firm and reveals that the estimated cost for remediating existing problems with RPAs is equal to your company's net income last year, due to many poorly designed, self-made, low-quality RPAs existing in numerous company departments - If controls are not built around RPA, an organization could face a huge number of software robots created in a short period of time, posing significant operational risks [44]. To prove this argument, Protiviti found through a study that among "RPA beginners", 61% of companies let individual department heads approve an RPA project. About 3% of people tried out cross-functional teams for project approval. 34% of RPA leaders still allow department heads to approve RPA projects themselves. Risk management is important in any project - it's no different with AI. The ability to create a plan and address existing and potential risks should be taken into account before adopting this new technology [58].

SH01 – Employee backlash, is mentioned in 3 publications. This risk happens when employees see RPA as a threat to their jobs, and of actively stalling or derailing implementation [56].

SH02 – IT not involved/uncooperative, is mentioned in 3 publications. This is a risk that happens when stakeholders take the initiative to implement RPA without consent of the IT department. On the other hand, it is also possible that the IT department does not find value in the implementation and makes it difficult to cooperate for the success of the implementation [23].

SH03 – Lack of visible progress and results, is mentioned in 3 publications. Stakeholder concern starts to rise when progress and results are not visible. The problem is that at this stage it may already be too late and correcting the implemented processes may mean additional costs [25].

SH04 – Poor stakeholder communication, is mentioned in 4 publications. Sometimes the way stakeholders use to communicate to developers the needs and requirements of a certain implementation project is through the creation of archaic documents like the PDD (Process Design Document) and SDD (Solution Design Document), where so much care and good practice is invested, but usually these archaic documents result in missing requirements and a poor and fragile bot [22].

SH05 – Difficulty managing organizational change, is mentioned in 4 publications. For companies to remain competitive in the market [47], sometimes stakeholders are forced to implement a change quickly, which can lead to difficulties in monitoring and managing this change due to unforeseen events, poor planning or lack of adherence by employees [59].

SH06 – Lack of experienced RPA resources, is mentioned in 6 publications. Being a recent technology, it is not always easy to find candidates with RPA skills and experience which can force stakeholders to employ people without the right competence for the complexity required [49].

SH07 – Difficulty identifying use cases to maintain a healthy automation pipeline, is mentioned in 3 publications. RPA requires detailed knowledge about the business process in which it is used - otherwise the expected performance improvements will not be realized [60].

SH08 – Inaccurate analysis, is mentioned in 3 publications. Considering that designed robots are typically deployed in production environments, where they interact with operational ISs (Information Systems), there is a lot of risk involved in building on an inaccurate analysis [61].

OE01 – Technical issues - Robots stop working or don't function as intended, is mentioned in 20 publications. RPA action is consistent, any error becomes a systemic and pervasive problem across the business process and dataset. Or, if there is a change in the business process, but the robot has not been modified to reflect this change, it may fail to execute or exhibit inaccuracy [9]. RPA failures can occur when changes happen in the system and are not anticipated [62].

OE02 – Not enough robots, is mentioned in 2 publications. It can mean that a process is not fully automated and part of it continues to work manually which makes it more prone to errors. It can also represent widespread bot shortages [25].

OE03 – Costly maintenance, is mentioned in 7 publications. RPA will revolutionize many careers that require additional training and skills. The demands for additional training vary from company to company. Additionally, organizations can find this difficult to provide with RPA software continuing to evolve. This means that it might not be realistic for organizations to rely on lower-skilled workers, who may not quickly adapt the new technology [63]. Another example is when the deal has been poorly executed and the cost of maintaining the bots is more expensive than the benefit it brings to the organization [64].

OE04 – Not optimizing processes before automating them, is mentioned in 7 publications. Improper process optimization will lead to inefficient automation. The main benefit of RPA is that it automates repetitive or precise tasks and provides opportunities to improve existing workflows [22].

OE05 – Incorrect process selection, is mentioned in 9 publications. It chooses the wrong process, applying RPA to a complex process that is expensive to automate and may not offer a meaningful return [46].

OE06 – Lack of scalability, is mentioned in 5 publications. It has been hard for companies to scale their RPA automation initiatives, as they become difficult to govern and manage when these automation systems are executed. This in turn makes it hard for them to execute their strategy and grow [62].

OE07 – Bad quality of data, is mentioned in 7 publications. RPA only works with structured data, otherwise it may have operational problems during its execution [65]. RPA robots are not perfect. They have limitations such as being unable to detect obvious errors (which humans can). If RPA bots aren't functioning properly, then any errors in their data will be transmitted and will greatly increase the probability of errors [52].

OE08 – RPA may hinder real process, is mentioned in 1 publication. RPA implementation when poorly designed or implemented can lead to execution errors that impair the normal functioning of the actual process [23].

OE09 – Lack of standardization, is mentioned in 2 publications. The lack of well-defined rules and process standardization makes it impossible to reuse use cases for other processes, which leads to more money and time spent [66].

OE10 – Poor documentation, is mentioned in 3 publications. It can lead to poor implementation design, which in turn will cause problems in the execution and maintenance of RPA. It also contributes to the lack of reusability of the processes already implemented due to lack of solid documentation [67].

OE11 – Human error, is mentioned in 5 publications. Numerous human errors can occur. An example of human error that can happen is when the developer, during the development phase, makes a mistake and configures something incorrectly, for example the bot takes data from the wrong place and consequently manipulates that data also in the wrong way. Then, in the testing phase, this small error is not detected and the bot is transported to the production environment. As the bot operates much faster than a human being, the error will be spread far and wide in a very fast way and can consequently damage and corrupt organizational data [68].

OE12 – Inefficient implementation of RPA, is mentioned in 8 publications. An inefficient implementation may be the consequence of the combination of several risks previously presented. An example of this risk, is when an organization after implementing several bots, the expected results are not in sight and did not match with expectations [44].

OE13 – Exception handling, is mentioned in 8 publications. Two different types of exceptions can be considered. Business Exception is when a previously defined process was not implemented or has some dependency that was not considered. Application/System Exception is for instance when a bot cannot connect to an external application to share information, or the bot is blocked by lack of permissions and cannot execute its task [69].

OE14 – Failure to monitor and identify changes to algorithms supporting RPA or the data sources and applications used for automation, is mentioned in 7 publications. A failure to monitor the execution of bots can lead to systematic errors that manipulate the information in the wrong way [70].

OE15 – Senior IT roles may become overburdened, is mentioned in 1 publication. As RPA can eliminate many operational work positions, it can increase the workload for senior IT managers to monitor and manage new systems in place. This extra work can strain resources and reduce employee morale, causing problems in attracting and retaining talent [35].

OE16 – Over-automating, is mentioned in 2 publications. When automation is identified as the primary solution to meet the need to automate processes rapidly, the rush to want to automate processes quickly leads to fragile automations that ultimately fail [22].

OE17 – Reinforcing bias, is mentioned in 1 publication. The risk with automating decision processes is that it eliminates the opportunity to consider what opportunities are being missed by requiring decisions to be based on strict criteria based on historical behavior. Consequently, in automating a process there can be a risk of creating an environment where outcomes are never questioned [71].

OE18 – Combine RPA with AI, is mentioned in 2 publications. Combining RPA with artificial intelligence capabilities can also raise challenges. For example, if machine learning (ML) is used to handle complex processes such as specific claims, the results are highly dependent on the data that the AI learns from. When the historical data fed into the ML algorithms, is of low quality, bad decisions and actions will be executed faster [12].

CM01 – Not building change management capability, is mentioned in 3 publications. Implementing RPA implies building a structure that allows for subsequent changes to processes, so that it is possible to carry out solid and consistent application maintenance without affecting the execution of the processes already implemented [25].

CM02 – Human Resources messaging not aligned, is mentioned in 3 publications. A lack of communication plan, executive buy-in, operational models, and catering to change management activities can lead to problems with alignment between processes and people, causing HR issues and delays in the long run. [38].

CM03 – Unclear roles, is mentioned in 4 publications. When the rules are not clear and well-defined, there is a risk that individual employees will interpret the use of RPA in different ways. It can also run the risk of an organisation holding on to a bad set of applications while it could be rethinking an opportunity to replace the legacy system that is supported by RPA [72].

CM04 – Lack of user know-how, is mentioned in 14 publications. An employee may think they will lose their job because automation will do their work [26]. The concept of RPA may not be understood [23]. The organization may face a major hurdle in implementing RPA due to lack of social acceptance from employees as they think it will impact the labor market and their jobs, thinking that they risk a cut in the number of jobs within the organization [13].

CM05 – Lack of communication plan, is mentioned in 7 publications. When changes are imposed, and these changes are not properly communicated to the whole organization, there will certainly be unexpected impacts on the execution of RPA, and errors may appear which in an initial phase will be more difficult to detect due to lack of information on the changes applied to a certain process [25].

CM06 – Lack of quality and control improvements, is mentioned in 8 publications. An organization must control the past and the present. Controllers may need to be reviewed because RPA results in modifications to policies and procedures. The need to apply new controllers must be assessed and also determine the obsolescence of previous controllers. Without these controls, RPA runs the risk of not keeping pace with change and incurring execution errors [55].

CM07 – Lack of formal process for assessing how source application changes affect bots that access them, is mentioned in 6 publications. Most RPA solutions need to be customized to suit your business. It doesn't pay for an organization to invest in implementation if the way the business operates will change dramatically in the future. Even small changes to your configuration can create significant disruptions to RPA bots [52].

CM08 – Lack of a formal and consistent process for requesting and implementing changes to bots, is mentioned in 7 publications. Failure to adopt a process that manages changes to RPA, along with the absence of documented dependencies of RPA on other software components, can result in unavailable service and processing errors [44].

CM09 – Lack of segregation of RPA development and production, is mentioned in 3 publications. The lack of segregation of RPA programs can make change difficult. When programs are not properly modularized it makes it more difficult to apply changes to a particular point in the process and also makes it more difficult to put that new block of code into production, because it may imply changing another process that did not need to be changed [56].

CM10 – Employee resistance to change, is mentioned in 5 publications. When processes changed faster than expected and the related bots did not work properly, creating many exceptions that employees had to deal with. This ended up significantly undoing the initial workforce reduction resulting again in additional work efforts and employee dissatisfaction. This could lead to resistance from employees to resume the correct functioning of the RPA [12].

CM11 – Drive change only by ROI perspective, is mentioned 4 publications. An RPA implementation driven only by the ROI perspective without a proper automation strategy also leads to significant problems because the other effects of the implementation are not being sufficiently considered. The lack of proper prioritization and implementation planning significantly limits business results [12].

CM12 – Regulatory risk, is mentioned in 6 publications. Ever-changing laws and regulations mean that RPA bots must be constantly monitored and changed according to government regulations [73]. If they are not updated, they may incur regulatory risks. Insufficiently tested and invalid algorithms used by bots can lead to financial losses (e.g. improper transaction recording, delayed payments) and affect the integrity, validity and accuracy of internal and external financial reporting. Currently, there are no regulatory standards for automated bots, which may result in bots inadvertently violating laws [49].

CM13 – Failing to Map Dependencies, is mentioned in 2 publications. The most common reason for an AI process to fail is if the interface changes. There are many risks associated with having RPA processes in your business, including failure to perform fully because of deficiencies with dependencies (both internal and external) [22].

MT01 – Underutilization of bots, is mentioned in 3 publications. Sometimes, the maturity of RPA projects in an organisation, gain too much confidence in their use, causing bots to be overused, leading to the effectiveness or profitability of their use becoming lower than it was supposed to be [69].

MT02 – Skills leakage/shortage, is mentioned in 8 publications. Assuming that the skills learned by business users are sufficient to put RPA into production can be dangerous [47]. Automating processes is an experience that requires continuous learning with training in testing processes, if this opportunity to practice is removed, the ability to make effective decisions will also be reduced [71].

MT03 – Lack of integration with new technologies, is mentioned in 7 publications. When an RPA project reaches a certain level of maturity, it runs the risk of not wanting to integrate new technologies so that there is no need to change the process, but this can make the process legacy over time [66].

MT04 – General lack of controls, is mentioned in 4 publications. After some time of implementing RPA, it is normal to question whether the bot is doing what it is supposed to do. This question may indicate that there is a lack of automated alerting tools for error handling. There needs to be continuous monitoring, even post a successful implementation, otherwise when bots fail it can represent many negative impacts for the organization [56].

MT05 – Lack of Business continuity preparedness, is mentioned in 3 publications. It is a common risk when there is no other platform or technology ready to take over the functions that the RPA was performing before it stopped working. For example, a company is unable to process customer requests for the third day in a row. The RPA managed the processing of all customer requests through an online platform that stopped working. Employees could no longer handle the workload due to the high number of customer requests. This shows that if the RPA is not properly covered by a business continuity programme, the failure of a single bot can result in a crisis situation in the company [44].

MT06 – Reputational damage, is mentioned in 3 publications. Existing controls should be reviewed and enhanced if necessary before introducing bots. Bots should be configured to generate exceptions and report errors to allow employees to take corrective action. Lack of adequate control over bot decisions, can induce reputational risk [44]. For example, an online news portal, starts a campaign against a company because the pricing of loan rates is biased. A strong correlation between loan rates and the customer's skin colour was identified in the course of a recent investigation by an independent internet user. In fact, loan applications are automatically processed by the newly developed cognitive RPA and the organisation cannot justify how the loan rate is calculated. Learning algorithms can pick up patterns or make decisions that are ethically unacceptable, and result in reputational damage for the organization [49].

MT07 – Lack of long-term sustainability, is mentioned in 2 publications. A couple of publications mentioned that RPA is already a lure for long-term work needed to digitize and make administrative processes more efficient, for example. As this work can be time-consuming and slow to carry out, there is a risk of focusing on quick fixes rather than getting it right from the start [52].

SO01 – Pick wrong advisors/partners or pick right advisors too late, is mentioned in 10 publications. Hard-to-identify damage and the lack of internal skills are only two of many factors that are contributing to excessive damage. Another example is choosing the wrong consulting partner- which can lead to data compliance risks [39].

SO02 – Cloud data / compliance risks, is mentioned in 11 publications. The introduction of robots presents a new set of regulatory risks which all businesses should consider. Neglecting to build compliance processes into an organization's RPA implementation process can lead to not meeting business requirements and KPIs. [55]. Failure to explain the results produced by RPA bots to regulators can result in penalties or even loss of license/authorization to operate in the market [44]. For example, in an organization, a report found that IT, marketing and finance departments were using RPA much more than any other department in the company.So the marketing team can automate the collection of customer data to send newsletters, but if the RPA effort does not include a mechanism for obtaining parental consent for their children's data, that is a compliance risk [58].

SO03 – Fails to determine what IT infrastructure is required to scale and protect the RPA processes, is mentioned in 2 publications. It happens when the outsourcing consultancy chosen to automate the processes of an organization, did not have the ability to choose a solid process base that would allow the spread of automation to other related processes [70].

SO04 – Contractual risks, is mentioned in 1 publication. There are now a lot of providers active in the RPA industry. This has led to a wide variety of products and services, from smaller companies to big corporations. These suppliers generally have less capacity for contractual risk-taking than do larger players with more financial strength and viable insurance arrangements. [73].

TS01 – Selecting the wrong tool, is mentioned in 8 publications. Due to the numerous automation tools offered by product and service providers, it can be difficult to choose the one best suited to the business process. For instance, some vendor features which claim they automate screen taking can produce errors, if they do not offer the full-screen automation techniques [39].

TS02 – Crowded vendor offerings, is mentioned in 3 publications. In such a competitive market, it can be difficult to choose the most suitable supplier due to the large number of offers on the market [25].

TS03 – The ease of getting RPA up and running, is mentioned in 3 publications. Robotic Process Automation vendors emphasize the ease of implementing their service. They also mention how quick and easy these tools are to use. The use of RPA can have many benefits, but there are some disadvantages. Complex environments need a little expertise to be able to take advantage of this fully [12]. Simply automating the workflows of individual employees in different ways is bad practice. It easily leads to a patchwork of redundant bots instead of automating end-to-end processes that bring far greater benefit to the organization [47].

LP01 – Unrealistic expectations, is mentioned in 9 publications. Believing that RPA alone will result in optimal ROI [47] or focusing more on the number of bots acquired than on the outcome that implementing RPA can bring [74]. An organization may also run the risk of wanting to implement processes that are not suitable for RPA. If your organization needs to process invoices, for example, it is best to use software that better understands and manages the data from the onset [52].

LP02 – Try to automate too much, is mentioned in 2 publications. Wanting to automate too many processes may not be efficient. It is easier to start an RPA project with simple processes and build up experience over time, rather than wanting to automate too much even before the project starts [25].

LP03 – Bad shortcuts – testing, documentation, etc, is mentioned in 8 publications. It is a frequent risk when the organization wants to skip planning steps or shortcut the path of certain processes. It also happens when the testing phase is run directly in the production environment, and this can put production at high risk [75].

LP04 – Underestimating human capital, implementation failure, is mentioned in 2 publications. It is critical that the IT department is involved in large-scale RPA implementations. Companies sometimes forget the IT knowledge and infrastructure required to maintain and adjust RPA bots. Business users can autonomously optimize simple workflows using AI tool's drag-and-drop menus. For enterprise deployments, however, IT expertise and administrative oversight are needed. [47].

LP05 – Views RPA as an IT project, not a business initiative, is mentioned in 1 publication. An RPA project should be seen as a business initiative to automate the processes of an organization, whether they are IT or non-IT processes. The IT department should be involved in the project, but it should not be considered that it is only an IT project, as you may be limiting the capability of RPA to one single department [47].

LP06 – Applies traditional software delivery methods to RPA, taking months to deploy when weeks is the norm, is mentioned in 1 publication. An organization should plan for continuous software delivery, rather than wanting to implement all automated processes at once, which turns out to be risky [47].

LP07 – No component reusability, is mentioned in 1 publication. When planning the implementation of an RPA project for certain projects, the possibility of implementing transversal modules should be considered, which will allow the future use of these modules for new process implementations, thus saving time and money for the organization by reusing the components that were previously developed [23].

LP08 – Legacy apps silos, is mentioned in 5 publications. When applications are outdated, processing errors can easily be detected because they may not support RPA execution. Legacy applications, too, typically lose application support. An organization also runs the risk of wanting to automate legacy application processes that will probably need to be upgraded in a short period of time, and this will mean changing all the existing RPA implementation, which will consequently cost the organization more time and money [59].

LP09 – Fast implementation, is mentioned in 2 publications. Rapid deployment can lead to organizations ignoring the need for full implementation protocols, accuracy and data versioning. Important steps can be overlooked or purposefully skipped [76].

LP10 – Very expensive implementation, is mentioned in 6 publications. While RPA is a very valuable piece of software that results in increased productivity, it is still very cost prohibitive for many organizations [35]. Some smaller organizations have been able to use RPA successfully, but even larger organizations may have problems justifying the move to RPA if cash flows are weak and they cannot meet the expense. Most AI-systems are expensive to customize and implement. They may be difficult to use for more complex tasks that require some degree of human judgement or creativity [51]. Implementing thousands of bots is much more expensive and takes much longer than organizations expected [77].

LP11 – Risk of redundancy, is mentioned in 1 publication. Although RPA can serve to eliminate redundant tasks practiced by humans, an organization may run the risk of mapping redundant processes that do not bring significant value that would justify automating that process [78].

SC01 – Data leakage, is mentioned in 9 publications. Without proper security measures, sensitive data that the RPA handles can be exposed to attackers, for example, credentials or customer data. There is a risk that the bot can be manipulated to transport the data out of the organization [40].

SC02 – Fraud, is mentioned in 7 publications. When a company plans to incorporate automation into one aspect of accounting, specifically accounts receivable, then it is necessary to fully understand each component of its process. Through an assessment, an employee may recognize a weakness in the entire process and manipulate data in an underhand manner - this may result in fraudulent activity [79].

SC03 – Lack of access management, is mentioned in 15 publications. RPA presents security problems if the level of regulation that applies to an organization is not considered. Deliberately unauthorized access can result in data leakage, and one could also mistakenly grant access to information that should have remained protected. Generally bots are configured and trained to never deviate from the same security policies that apply to a human user, but a failure in access management, can allow the bot free access to the entire network and can compromise an organization's compliance rules [35].

SC04 – Compromised data, is mentioned in 10 publications. Sometimes a bot needs to access and manipulate confidential data in order to complete its task. With that data being compromised, it poses an additional security risk to the organization. It is necessary to have well-defined security policies to avoid fraudulent activities or data leakage [62].

SC05 – Inappropriate access to sensitive data, is mentioned in 11 publications. It can happen that a bot is misconfigured and improperly accesses sensitive data and creates compliance conflicts within the organization. There is also the scenario where the bot purposely needs access to sensitive data to complete its tasks and an employee takes advantage of the misconfigured bot's access to obtain information that should not be allowed to be viewed or even extract that data for personal benefit [80].

SC06 – Abuse of administration privileges, is mentioned in 8 publications. The abuse of administrator privileges can happen in several scenarios. Either the administrator takes advantage of their ability to access sensitive processes or data and uses that information for their own benefit by accessing privileged information or even selling data to other organizations, or they may, for example, grant improper access to other employees to give them an advantage over other employees in the organization [81].

SC07 – External threats, is mentioned in 14 publications. If the bot is not well protected, a hacker or group of hackers can break into the system and access confidential data [82]. In the same way that cyber-attacks can damage organizational assets, a bot with weak security can also be damaged. Security testing and risk assessments should often be done on a regular and systematic basis [55]. There is also the scenario, where a hacker configures the organization's own RPA bot to damage or extract data. These events may be aimed at just damaging organization assets or it may serve to ransom the sensitive data in exchange for large amounts of money [49].

SC08 – Internal threats, is mentioned in 6 publications. It can happen when an internal employee manipulates or trains a bot for malicious purposes [82]. For example, data from the system that manages customer relationship data (CRM) was stolen and then sold on the black market. After a security investigation, they concluded that the root cause of the data breach was an internal fraud, created from the back-office department caused by a former employee using RPA to extract the data. The inability to establish unified, secure and efficient IAM practices resulted in an internal attack [44].

SC09 – Poor design, is mentioned in 5 publications. A poorly designed RPA bot, may inadvertently expose confidential data, personal information, electoral records, financial details, for example, due to a bot execution done on a public network [53].

SC10 – Unsecure data management, is mentioned in 9 publications. If a bot doesn't encrypt data before sending it to the cloud or if that data is exposed in some other way, it can be accessed by someone else. It could also get its information decrypted by another entity [53]. Another example is when customers of a bank started receiving bank statements from other people by email. Since this information is confidential and personal, the customers asked the bank staff if their data was sent to other customers. Subsequently it was discovered that it was an RPA bot that was incorrectly distributing the bank statements. This unintentional disclosure of confidential data occurred due to the lack of insecure data management that the RPA was handling [44].

SC11 – Network vulnerability, is mentioned in 13 publications. An organization's own network may be compromised, and this will naturally compromise the execution of RPA bots as well. For example, an update of a software widely used by a bot needs a stable connection to the network and cannot update properly due to continuous connection failures, which consequently compromise the RPA execution [44].

SC12 – Denial-of-service interruptions, is mentioned in 3 publications. If too many bots perform too many activities in succession too quickly, the network can become so overloaded that it causes service interruptions that can consequently cause security violations [82].

SC13 – Lack of bot accountability relating to security, privacy, and compliance requirements, is mentioned in 5 publications. A bot has to represent its role in compliance with security, otherwise the lack of accountability of the bot can bring difficulties in discovering the origin of some vulnerability that has happened inside the organization [53].

SC14 – Remote code execution, is mentioned in 1 publication. Executing code remotely must take into account several security aspects, both at the data encryption level and at the network or cloud protection level. Otherwise, compliance issues can compromise the execution of RPA bot code [83].

4.4. RPA Risks Synthesis

This section aims to list and summarise the contributions of this study, as it sought to explain underlying features of RPA, establishing some of the weaknesses or expectations of its evolution as an automation tool in management.

In this line of thought, a solid basis was developed, which may facilitate future developments towards the creation of a robust data collection instrument for similar studies.

The collected perceptions may themselves provide signals for the improvement of this instrument, as the obtained testimonies are grounded by relevant professional experience of individuals with daily contact with RPA.

Therefore, from a theoretical and practical perspective, this research contributes scientifically to deepen the knowledge of the RPA universe, and its main risks during its implementation since the respective research is pioneering because it reflects a very specific technological component in scientific literature and, consequently, recent in the market. Furthermore, as presented in Table 7, cybersecurity and operational risks prove to be the most impactful in the RPA area for a big reason:

The respective Security and Operational Risk Groups present the highest number of mentions in the data extraction. Thus, it demonstrates that these are risks that have been materialized and highlighted with greater frequency among potential specialists involved in matters related to RPA, as can be seen in Figure 15.

TABLE 7 – LIST OF MAIN GROUPS OF RPA RISKS IDENTIFIED BY NUMBER OF MENTIONS OVER THE YEARS

	2016	**2017**	**2018**	**2019**	**2020**	**2021**	**Total**
Strategy Risks	0	4	11	12	13	8	**48**
Stakeholders buy-in Risks	0	4	4	8	5	8	**29**
Operation and Execution Risks	2	4	21	28	25	17	**97**
Change Management Risks	1	7	15	17	19	13	**72**
Maturity Risks	0	3	6	6	11	4	**30**
Sourcing Risks	0	4	7	5	4	4	**24**
Tool Selection Risks	0	2	3	5	3	1	**14**
Launch/project Risks	1	9	3	10	9	6	**38**
Security Risks	1	0	18	19	41	36	**115**
Total	**5**	**37**	**88**	**110**	**130**	**97**	**467**

Interestingly, as shown in Figure 12, these same risks were cited in recent years, this helps to prove that in the face of the exponential growth and use of RPA technologies in recent times these same risks represent a significant impact on the use and implementation of RPA.

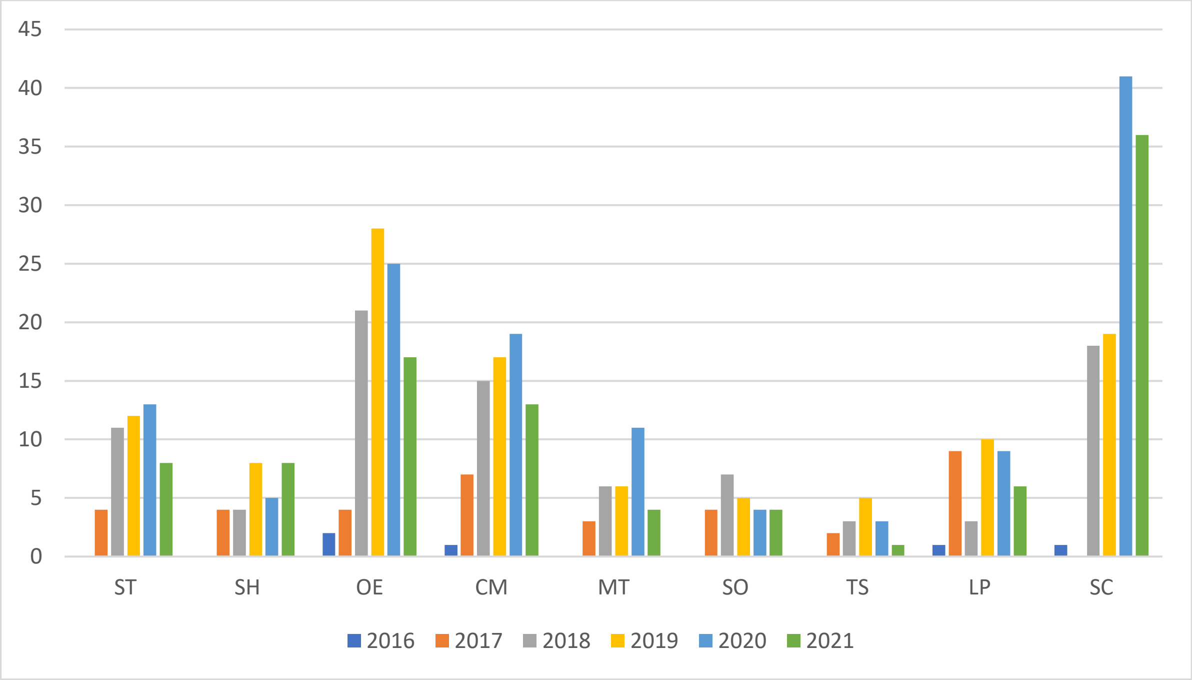

FIGURE 12 - NUMBER OF PUBLICATIONS PER RISK CATEGORY OVER THE YEARS

On the practical contributions, this study is revealing from two main perspectives. Firstly, it not only helps industry experts identify the potential risks they face, but also helps them structure new implementations by knowing how to identify and avoid risks.

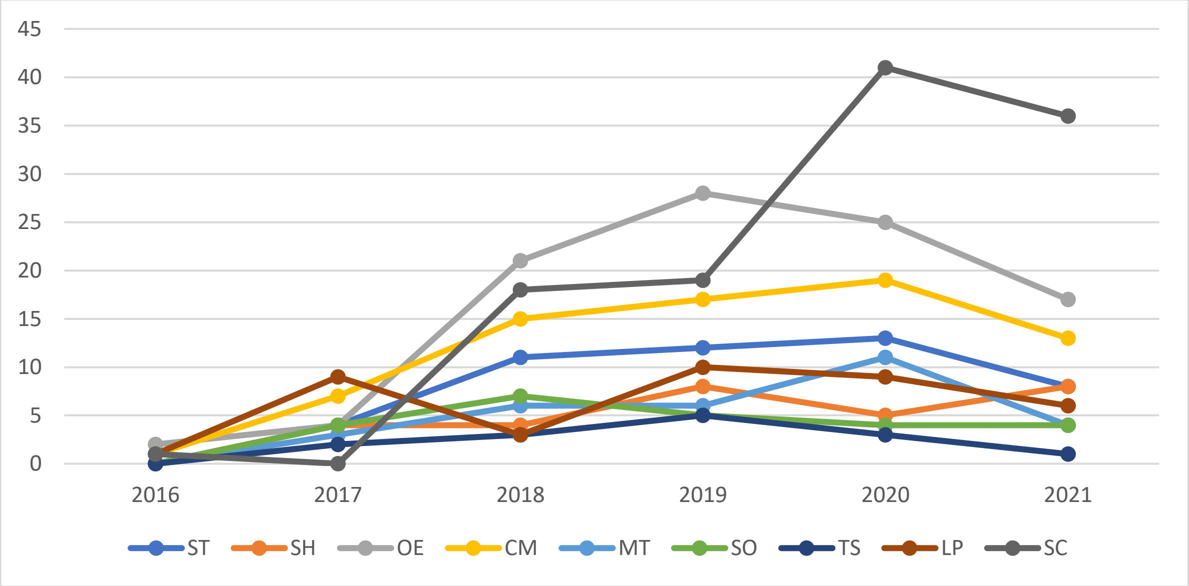

FIGURE 13 - DISTRIBUTION OF MENTIONS PER GROUP OF RISK OVER THE YEARS

4.5. Framework proposal

RPA in companies is increasingly a key strategy to obtain competitive advantage in the market, however, like any new technology, the implementation of this resource requires attention from experts working with automation.

Thus, as mentioned in previous chapters this study aims to identify the Risks of RPA, having as main objective to contribute scientifically in mapping them, to help professionals or future researchers to mitigate potential impacts throughout the cycle of implementation and maintenance of RPA, and consequently improve the potential of this automation.

In order to clarify the concepts and dimensions exposed in this section dedicated to the Framework two views are presented: first a Framework proposed in a macro view centralized in the different dimensions of analysis is followed, second a more detailed view focused on the various concepts under study - the risks and derivatives.

In this way, the concepts under study were mapped into a framework allowing for the systematization in a logical manner of the various dimensions under analysis based on the fusion and adaptation of other existing models in the scientific community.

As presented in Figure 13, the framework is outlined in four layers of the phenomenon under study. It is important to highlight that the various layers demonstrated are interconnected in a sequential manner. This structure is based on the findings of the MLR, reflected in the general research objective:

Thus, in the **first layer** the **strategy phase** is proposed where it includes three types of risks, namely, strategic risks, stakeholder buy-in risks and sourcing and tool selection risks.

Following this, **the second layer** is dedicated to the **implementation phase** which includes the project / launch risks.

In the **third layer**, **operational and execution phase**, which covers operational / execution risks and security risks.

And finally, the **fourth layer** focuses on the **post execution phase** which integrates change management risks and maturity risks.

Assuming that this first layer takes into consideration an adaptation of the framework proposed in the [84] article.

Additionally, two more dimensions of analysis are mapped, such as factors and the crosscutting risks. In fact, some authors categorise these variables as risks, but given the definition of this concept set out in the first section of this study, and upon reflection, they do not fit the respective meaning. Therefore, they were categorised as cause-effect factors, i.e. factors which potentiate risk. It was also considered relevant to highlight the risks that are crosscutting to several layers, since they can impact on any of the four layers.

It is important to highlight that before conceptualizing the Framework, this research focused on the MLR methodological process in the identification and categorization of potential RPA risks. The reflection of this model went through a careful analysis of each risk in which it was filtered and directed between the exposed layers and variables, as can be seen in the more detailed view of the model in Figure 14.

It is important to note that the risks and factors have been recategorized and adapted in the layers currently designed in the framework and have no connection to the categorisation of the main groups of risks identified in the previous sections, prior to this respective filtering.

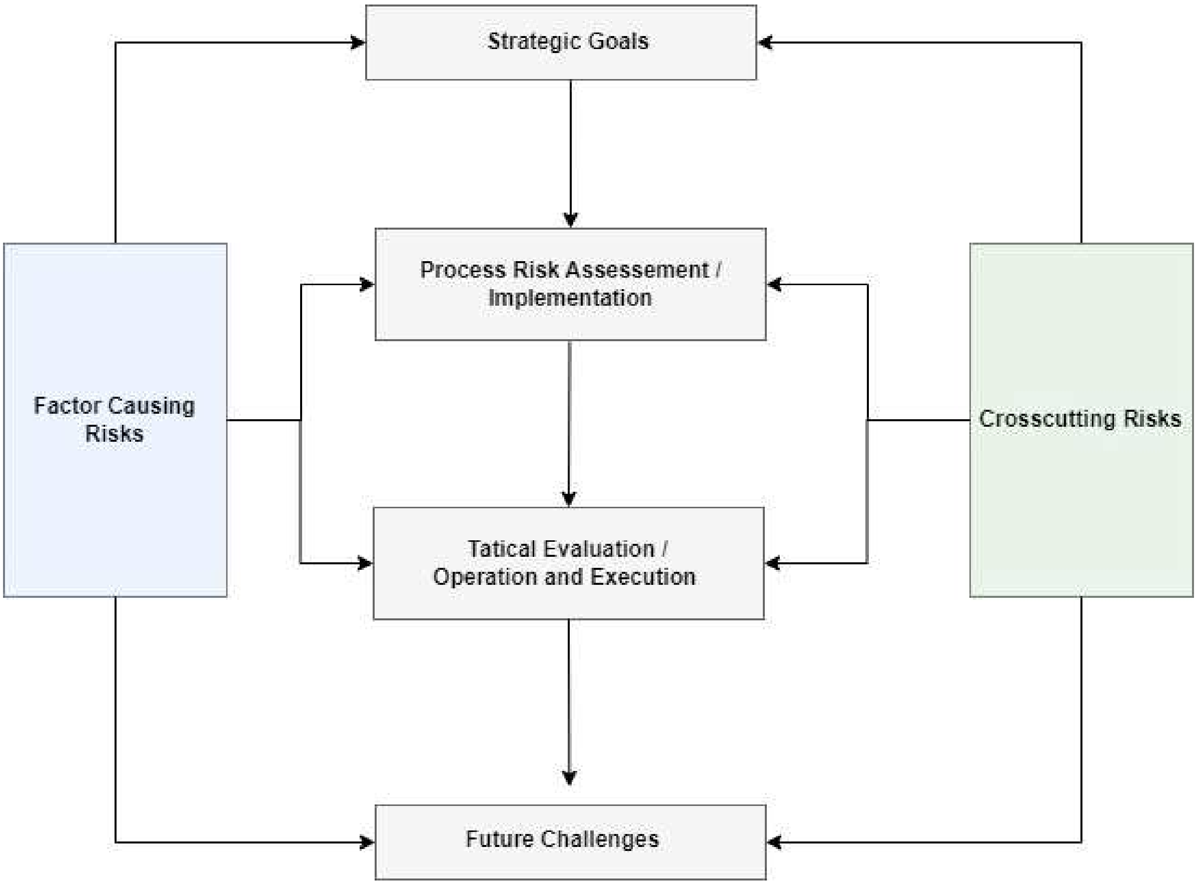
Strategic Goals
Process Risk Assessement / Implementation
Factor Causing Risks
Crosscutting Risks
Tatical Evaluation / Operation and Execution
Future Challenges

FIGURE 14 - MARCO VIEW OF FRAMEWORK [84]

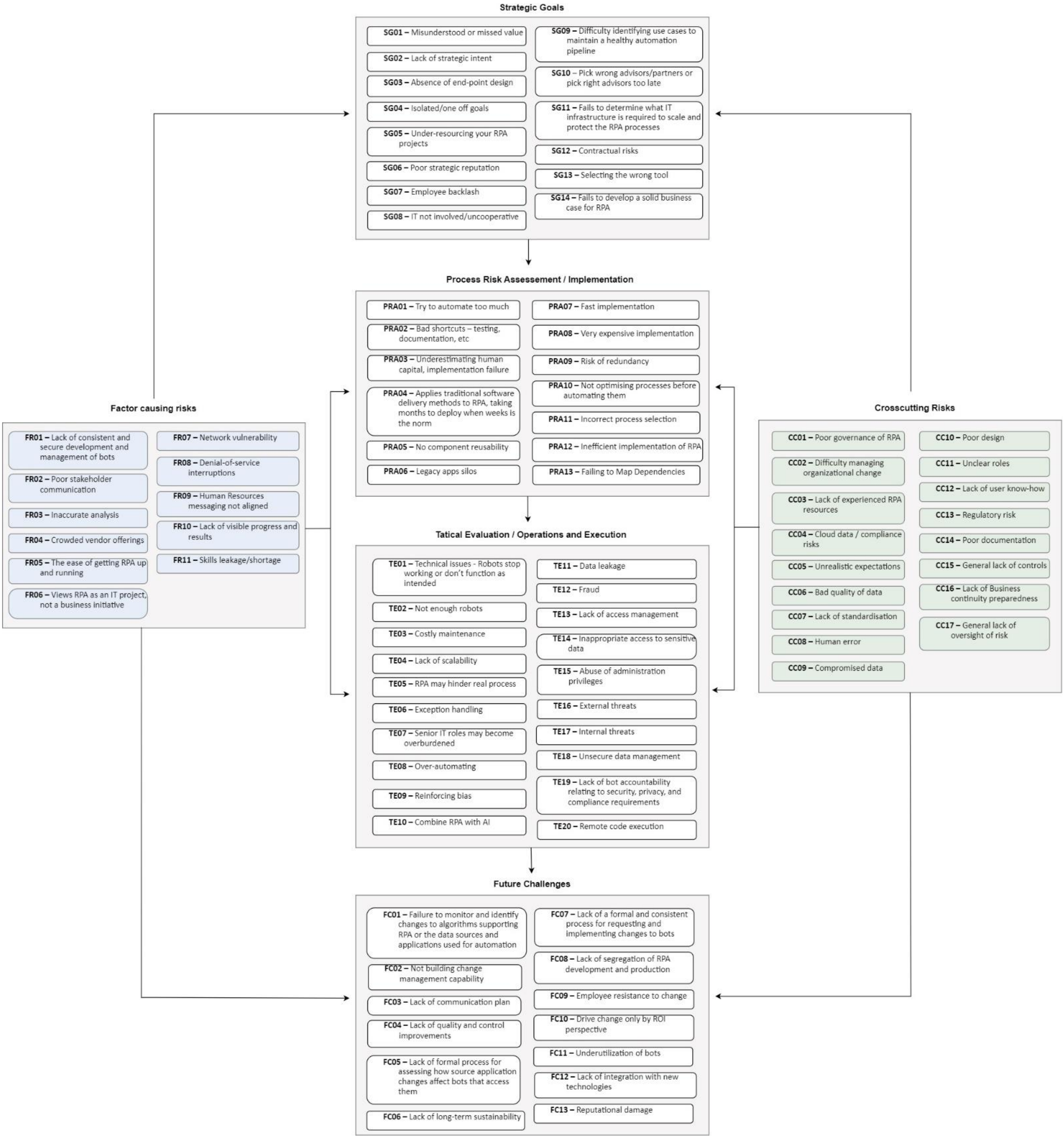
Strategic Goals
SG01 – Misunderstood or missed value
SG02 – Lack of strategic intent
SG03 – Absence of end-point design
SG04 – Isolated/one off goals
SG05 – Under-resourcing your RPA projects
SG06 – Poor strategic reputation
SG07 – Employee backlash
SG08 – IT not involved/uncooperative
SG09 – Difficulty identifying use cases to maintain a healthy automation pipeline
SG10 – Pick wrong advisors/partners or pick right advisors too late
SG11 – Fails to determine what IT infrastructure is required to scale and protect the RPA processes
SG12 – Contractual risks
SG13 – Selecting the wrong tool
SG14 – Fails to develop a solid business case for RPA
Process Risk Assessement / Implementation
PRA01 – Try to automate too much
PRA02 – Bad shortcuts – testing, documentation, etc
PRA03 – Underestimating human capital, implementation failure
PRA04 – Applies traditional software delivery methods to RPA, taking months to deploy when weeks is the norm
PRA05 – No component reusability
PRA06 – Legacy apps silos
PRA07 – Fast implementation
PRA08 – Very expensive implementation
PRA09 – Risk of redundancy
PRA10 – Not optimising processes before automating them
PRA11 – Incorrect process selection
PRA12 – Inefficient implementation of RPA
PRA13 – Failing to Map Dependencies
Factor causing risks
FR01 – Lack of consistent and secure development and management of bots
FR02 – Poor stakeholder communication
FR03 – Inaccurate analysis
FR04 – Crowded vendor offerings
FR05 – The ease of getting RPA up and running
FR06 – Views RPA as an IT project, not a business initiative
FR07 – Network vulnerability
FR08 – Denial-of-service interruptions
FR09 – Human Resources messaging not aligned
FR10 – Lack of visible progress and results
FR11 – Skills leakage/shortage
Crosscutting Risks
CC01 – Poor governance of RPA
CC02 – Difficulty managing organizational change
CC03 – Lack of experienced RPA resources
CC04 – Cloud data / compliance risks
CC05 – Unrealistic expectations
CC06 – Bad quality of data
CC07 – Lack of standardisation
CC08 – Human error
CC09 – Compromised data
CC10 – Poor design
CC11 – Unclear roles
CC12 – Lack of user know-how
CC13 – Regulatory risk
CC14 – Poor documentation
CC15 – General lack of controls
CC16 – Lack of Business continuity preparedness
CC17 – General lack of oversight of risk
Tatical Evaluation / Operations and Execution
TE01 – Technical issues - Robots stop working or don't function as intended
TE02 – Not enough robots
TE03 – Costly maintenance
TE04 – Lack of scalability
TE05 – RPA may hinder real process
TE06 – Exception handling
TE07 – Senior IT roles may become overburdened
TE08 – Over-automating
TE09 – Reinforcing bias
TE10 – Combine RPA with AI
TE11 – Data leakage
TE12 – Fraud
TE13 – Lack of access management
TE14 – Inappropriate access to sensitive data
TE15 – Abuse of administration privileges
TE16 – External threats
TE17 – Internal threats
TE18 – Unsecure data management
TE19 – Lack of bot accountability relating to security, privacy, and compliance requirements
TE20 – Remote code execution
Future Challenges
FC01 – Failure to monitor and identify changes to algorithms supporting RPA or the data sources and applications used for automation
FC02 – Not building change management capability
FC03 – Lack of communication plan
FC04 – Lack of quality and control improvements
FC05 – Lack of formal process for assessing how source application changes affect bots that access them
FC06 – Lack of long-term sustainability
FC07 – Lack of a formal and consistent process for requesting and implementing changes to bots
FC08 – Lack of segregation of RPA development and production
FC09 – Employee resistance to change
FC10 – Drive change only by ROI perspective
FC11 – Underutilization of bots
FC12 – Lack of integration with new technologies
FC13 – Reputational damage

FIGURE 15 - DETAILED VIEW OF FRAMEWORK [84]

Section 5 – Conclusion

This research is based on an MLR on the emerging topic of robotic process automation, which takes into account publications spanning from 2016 to 2021. In this sense, it adds significant contributions to the scarce academic literature in this evolving field of the RPA universe and associated risks. As such, this study provides a strong starting point for the integration of knowledge of risks arising from RPA use and implementation.

Due to the lack of comparative and integrative studies, and with the use of grey literature in conjunction with academic literature, it is possible to ensure that the content under study is recent and up-to-date across various fields of endeavour, whether from an organisational, business, academic and professional perspective. Thus, this study proposes a unified definition of the variables under study, including the identified RPA risks in a total list of 88 risks integrated into 9 main risk groups.

Throughout this research, it was also found in the MLR results that RPA risks were referred to with a higher incidence in the grey literature rather than in the academic literature. This not only proves that this subject is a pioneering study in the scientific communities, but it is also an almost unprecedented investigation. It was also found that the most referenced risks are the most recent Security and Operational related risks which in fact, largely resulted from the grey literature.

During Framework conceptualization, this research focused on identifying and recategorizing potential RPA risks, going through a careful analysis of each risk. In this sense, each risk was filtered and directed between five layers adapted from a model proposed in the [84] article. In this way, it is important to highlight that the risks and factors were reorganized in the layers designed in the framework, having no connection to the main groups of risks identified in the first part of this study. Moreover, after this exhaustive analysis it was found that some of the highlighted risks were crosscutting to the various main risk groups, and other risks that were recategorized as factors that cause the risk.

In terms of the study contributions from a theoretical point of view, this research helps researchers to inform themselves about a conceptual view of RPA risks in their use and implementation. Secondly, from a practical point of view, it helps industry experts beyond knowledge about the risks they face, which ones have the greatest impact and thus conceptualise new ways of implementation and ways to avoid them.

Like all studies, this one also has some limitations. Firstly, the use of grey literature to support a scientific statement may be debatable, but it is justified by the peculiarities of this field: the scarcity of adequate academic literature on RPA; the delay in applying academic research to real-world situations; and the role that grey literature plays in providing contextual information complementary to academic literature.

5.1. Threats to validity

Although this research takes into consideration the care with scientific and methodological rigor, there are some inherent limitations that will be exposed taking into account the defined qualitative research. This is because, the fact that this study was based on multivocal literature ends up being a limitation because many of the results of the exposed information do not go through the rigor of peer review to which academic research is usually subjected.

Here, it was chosen to create the review approach following the suggestions of Garousi et al. [27] and perform each step using this method to lessen the impact of this threat. Data extraction specifically uses organised processes and logistics such as distinct traceability links between acquired data and primary sources. Over-reliance on Google search of the study ultimately limits the research results.

However, to refine the search results by writing code in Python the results obtained from Google search are not user-specific but general, thus solving the problem of consistency in the returned results because Google returns custom results that are tailored differently for each user based on their previous search history and preferences.

Indeed, there is a need to raise awareness with this type of search in order to make empirical research more accessible to systematic reviewers.

Furthermore, only articles in English were included as references, restricting the scope of other studies in other languages.

Furthermore, as 20.56% of the publications in the grey literature are written by vendors offering RPA solutions or other consultancy services that support organisations in these same solutions, they end up presenting an approach that highlights or outlines the benefits and advantages rather than their risks and disadvantages.

5.2. Future Work

Once the major groups and RPA risks have been identified, as future research it would be interesting to deepen how each risk can be mitigated. In addition, it could also contribute to the scientific community to explore ways to reduce the respective risks or security solutions.

Given the rapid digital development, namely this technology combined with RPA processes, it is recommended that new reviews of the academic and grey literature are continuously investigated calling for an update of the state of the art of the respective subject.

Furthermore, literature assessment is subject to inherent subjectivity and thus should be treated accordingly since further research will be required to explore the subject matter. In this sense, it is suggested to further investigate this theme with the particularity of a differentiating data collection, opting for primary data as the research method based on both literatures.

References

[1] C. P. Lok, “Critical Success Factors for Robotic Process Automation Implementation,” p. 6, 2021.

[2] T. Kyheröinen, “Implementation of Robotic Process Automation to a Target Process-a Case Study,” p. 75, 2018, [Online]. Available: https://aaltodoc.aalto.fi/bitstream/handle/123456789/31518/master_Kyheröinen_Tuomas_2018.pdf?sequence=1&isAllowed=y.

[3] F. Hartmann, “Evolving Digitisation: Chances and Risks of Robotic Process Automation and Artificial Intelligence for Process Optimisation Within the Supply Chain,” no. July, 2018.

[4] J. B. (2020) Santos, F., Pereira, R. & Vasconcelos, “Towards Robotic Process Automation implementation: An end-to-end perspective,” no. 351, 2020.

[5] B. Van den Oever, “Method for estimating the impact of Robotic Process Automation implementations on business processes.,” 2020.

[6] C. Stamford, “Gartner Says Worldwide RPA Software Spending to Reach $2.9 Billion in 2022,” 2022. https://www.gartner.com/en/newsroom/press-releases/2022-08-1-rpa-forecast-2022-2q22-press-release (accessed Oct. 06, 2022).

[7] A. Meironke and S. Kuehnel, “Association for Information Systems Association for Information Systems AIS Electronic Library (AISeL) AIS Electronic Library (AISeL) How to Measure RPA’s Benefits? A Review on Metrics, Indicators, How to Measure RPA’s Benefits? A Review on Metrics, Indic,” 2022, [Online]. Available: https://aisel.aisnet.org/wi2022/bpm/bpm/5.

[8] C. M. G. Martins, H. Mamede, and M. L. B. M. da Silva, “Robotic Process Automation A Lean Approach to RPA Information Systems and Computer Engineering Examination Committee,” no. November, 2018.

[9] PwC, “Robotic process automation : A primer for internal audit professionals,” *Pwc*, pp. 1–4, 2018, [Online]. Available: https://www.pwc.com/sg/en/publications/assets/ra-robotic-process-automation-for-ia.pdf.

[10] F. Kosi, “Robotic Process Automation (RPA) and Security,” pp. 1–36, 2019.

[11] B. A. Kitchenham, “Systematic review in software engineering: where we are and where we should be going,” *Proc. 2nd Int. Work. Evidential Assess. Softw. Technol. - EAST ’12*, p. 1, 2012, [Online]. Available: http://dl.acm.org/citation.cfm?doid=2372233.2372235.

[12] M. Kirchmer and P. Franz, "Value-Driven Robotic Process Automation (RPA): A Process-Led Approach to Fast Results at Minimal Risk," *Lect. Notes Bus. Inf. Process.*, vol. 356, pp. 31–46, 2019, doi: 10.1007/978-3-030-24854-3_3.

[13] A.-M. Zaharia-Radulescu, C. L. Pricop, D. Shuleski, and A. C. Ioan, "RPA and the future of workforce," *Proc. Int. Manag. Conf.*, vol. 11, no. 1, pp. 384–392, 2017.

[14] J. G. Enriquez, A. Jimenez-Ramirez, F. J. Dominguez-Mayo, and J. A. Garcia-Garcia, "Robotic Process Automation: A Scientific and Industrial Systematic Mapping Study," *IEEE Access*, vol. 8, no. February, pp. 39113–39129, 2020, doi: 10.1109/ACCESS.2020.2974934.

[15] H. Sallet, "Simplified literature review on the applicability of process mining to RPA," 2021, Accessed: Oct. 24, 2021. [Online]. Available: https://www.lume.ufrgs.br/handle/10183/223236.

[16] L. Ivančić, D. Vugec, … V. V.-C. on B. P., and U. 2019, "Robotic process automation: systematic literature review," *Springer*, 2019, Accessed: Oct. 23, 2021. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-30429-4_19.

[17] T. Taulli, "The Robotic Process Automation Handbook," *Robot. Process Autom. Handb.*, 2020, doi: 10.1007/978-1-4842-5729-6.

[18] R. Martin, J. Flaherty, and K. Hansen, "How automation is evolving the role of Internal Audit in Healthcare Robotics Process Automation : How automation is evolving the role of Internal Audit in Healthcare," 2019.

[19] T. R. Eikebrokk and D. H. Olsen, "Robotic Process Automation and Consequences for Knowledge Workers; a Mixed-Method Study," *Responsible Des. Implement. Use Inf. Commun. Technol.*, vol. 12066, p. 114, 2020, doi: 10.1007/978-3-030-44999-5_10.

[20] T. Taulli, *The Robotic Process Automation Handbook*. .

[21] M. Gotthardt, D. Koivulaakso, O. Paksoy, C. Saramo, M. Martikainen, and O. Lehner, "ACRN Journal of Finance and Risk Perspectives Current State and Challenges in the Implementation of Smart Robotic Process Automation in Accounting and Auditing," *ACRN J. Financ. Risk Perspect.*, vol. 9, pp. 90–102, 2020, doi: 10.35944/jofrp.2020.9.1.007.

[22] blueprint, "7 Hidden Risks of Automation Design in Business | Blueprint," Jan. 27, 2021. https://www.blueprintsys.com/blog/rpa/7-hidden-risks-automation-design (accessed Jun. 11, 2022).

[23] D. Kedziora, "Robotic Process Automation (RPA) Implementation Drivers: Evidence of Selected Nordic Companies," *Issues Inf. Syst.*, vol. 22, no. 2, pp. 21–40, 2021, doi:

10.48009/2_iis_2021_21-40.

[24] W. Van der Aalst, M. Bichler, and A. Heinzl, “Robotic process automation,” 2018, Accessed: Oct. 22, 2021. [Online]. Available: https://link.springer.com/article/10.1007/s12599-018-0542-4.

[25] M. Lacity and L. Willcocks, *Robotic Process Automation and Risk Mitigation: The Definitive Guide*. SB Publishing, 2017.

[26] D. Wright, D. Witherick, and M. Gordeeva, “The robots are ready. Are you? Untapped advantage in your digital workforce,” *Deloitte Dev. LLC*, p. 24, 2018, [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology/deloitte-robots-are-ready.pdf.

[27] V. Garousi, M. Felderer, and M. V. Mäntylä, “Guidelines for including grey literature and conducting multivocal literature reviews in software engineering,” *Inf. Softw. Technol.*, vol. 106, pp. 101–121, 2019, doi: 10.1016/j.infsof.2018.09.006.

[28] V. Garousi, M. Felderer, and M. V. Mäntylä, “The need for multivocal literature reviews in software engineering,” pp. 1–6, 2016, doi: 10.1145/2915970.2916008.

[29] R. Amaro, R. Pereira, and M. Mira, “DevOps Capabilities and Practices : A Multivocal Literature Review,” pp. 1–19.

[30] A. Pokhrel, V. Katta, and R. Colomo-Palacios, “Digital Twin for Cybersecurity Incident Prediction: A Multivocal Literature Review,” *Proc. - 2020 IEEE/ACM 42nd Int. Conf. Softw. Eng. Work. ICSEW 2020*, pp. 671–678, 2020, doi: 10.1145/3387940.3392199.

[31] R. T. Ogawa and B. Malen, “Towards Rigor in Reviews of Multivocal Literatures: Applying the Exploratory Case Study Method,” *Rev. Educ. Res.*, vol. 61, no. 3, pp. 265–286, 1991, doi: 10.3102/00346543061003265.

[32] R. M. D. Amaro, R. Pereira, and M. Mira da Silva, “Capabilities and Practices in DevOps: A Multivocal Literature Review,” *IEEE Trans. Softw. Eng.*, pp. 1–24, 2022, doi: 10.1109/TSE.2022.3166626.

[33] J. Mitlohner, S. Neumaier, J. Umbrich, and A. Polleres, “Characteristics of open data CSV files,” *Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016*, vol. 838, pp. 72–79, 2016, doi: 10.1109/OBD.2016.18.

[34] T. Torlone, R. Howell, F. Ip, and A. Mahajan, “Ease of deployment,” *PwC*, pp. 1–8, 2016.

[35] Hugo Ciopages, “Robotic Process Automation: The opportunity, risks and rewards,”

Nov. 02, 2016. https://www.ciopages.com/robotic-process-automation/ (accessed Jun. 04, 2022).

[36] L. Willcocks, M. Lacity, and A. Craig, "Robotic process automation: Strategic transformation lever for global business services?," *J. Inf. Technol. Teach. Cases*, vol. 7, no. 1, pp. 17–28, 2017, doi: 10.1057/s41266-016-0016-9.

[37] N. Jain, "The risk of RPA implementation and how to mitigate it," Sep. 2020. https://www.capgemini.com/2020/09/the-risk-of-rpa-implementation-and-how-to-mitigate-it/ (accessed Jan. 09, 2022).

[38] X. Liao, "Top 8 risks associated with RPA and how to mitigate them," Jan. 22, 2019. https://www.joltag.com/blog/top-8-risks-associated-with-rpa-and-how-to-mitigate-them (accessed Jan. 09, 2022).

[39] T. Arun, "Robotic Process Automation (RPA): Risks and Controls | by Arun Thomas | Medium," Mar. 11, 2020. https://medium.com/@netsentries/robotic-process-automation-rpa-risks-and-controls-9afb96f7fcb3 (accessed Apr. 26, 2022).

[40] M. Sakpal, "How to Ensure Robotic Process Automation Security," Mar. 25, 2021. https://www.gartner.com/smarterwithgartner/4-steps-to-ensure-robotic-process-automation-security (accessed Jan. 09, 2022).

[41] K. Casey, "Robotic Process Automation (RPA): What you need to know about security | The Enterprisers Project," Jul. 09, 2020. https://enterprisersproject.com/article/2020/7/rpa-robotic-process-automation-security (accessed Apr. 26, 2022).

[42] J. Kaur, "Understanding Robotic Process Automation in Cybersecurity," Feb. 16, 2021. https://www.xenonstack.com/insights/rpa-security-risk-management (accessed May 08, 2022).

[43] J. Juttmann and M. van Doesburg, "Robotic Process Automation: how to move on from the proof of concept phase? - Compact," 2018. https://www.compact.nl/articles/robotic-process-automation-how-to-move-on-from-the-proof-of-concept-phase/ (accessed May 27, 2022).

[44] O. Pluzhnikov, "Top 10 security risks of RPA," *eleks*, 2020.

[45] S. Szalony, P. Salkin, and K. Sewell, "The 3 Rs of Finance Automation: RPA, Risk, Rewards - WSJ," Nov. 20, 2019. https://deloitte.wsj.com/articles/the-3-rs-of-finance-automation-rpa-risk-rewards-01574283372 (accessed May 27, 2022).

[46] KPMG, "Managing risks of the growing RPA jungle," p. 14, 2018, [Online]. Available: https://assets.kpmg/content/dam/kpmg/in/pdf/2018/12/Managing-risks-the-growing-

RPA-jungle.pdf.

[47] L. Tucci, “Ultimate Guide to RPA (Robotic Process Automation),” Mar. 17, 2021. https://www.techtarget.com/searchcio/Ultimate-guide-to-RPA-robotic-process-automation (accessed Apr. 18, 2022).

[48] N. Joshi, “Leverage RPA, But Plan For Its Inherent Risks, Too!,” Jun. 28, 2019. https://www.forbes.com/sites/cognitiveworld/2019/06/28/leverage-rpa-but-plan-for-its-inherent-risks-too/?sh=58aebc2a11d1 (accessed Jan. 09, 2022).

[49] D. Jędrzejka, “Robotic process automation and its impact on accounting,” *Zesz. Teoretyczne Rachun.*, vol. 2019, no. 105 (161), pp. 137–166, 2019, doi: 10.5604/01.3001.0013.6061.

[50] A. Katara and Z. Rashid, “Risk Management Magazine - Robotic Process Automation for Risk and Compliance,” Mar. 20, 2018. http://www.rmmagazine.com/2018/03/20/robotic-process-automation-for-risk-and-compliance/ (accessed Jan. 11, 2022).

[51] J. Frankenfield, “Robotic Process Automation (RPA) Definition,” Feb. 14, 2017. https://www.investopedia.com/terms/r/robotic-process-automation-rpa.asp (accessed Jun. 04, 2022).

[52] P. Holmlund, “The pros and cons of RPA: Is it the best choice for your business? | Qvalia,” May 06, 2020. https://qvalia.com/blog/the-pros-and-cons-of-rpa-is-it-the-best-choice-for-your-business/ (accessed Jun. 15, 2022).

[53] J. Schatz, “Considering RPA? Make sure you understand the security implications - GCN,” Dec. 18, 2019. https://gcn.com/cloud-infrastructure/2019/12/considering-rpa-make-sure-you-understand-the-security-implications/298178/ (accessed Apr. 21, 2022).

[54] i-SCOOP, “Robotic Process Automation (RPA): definition, benefits and usage,” 2020. https://www.i-scoop.eu/robotic-process-automation-rpa/ (accessed May 04, 2022).

[55] M. Bednarz, “7 Keys to Successful Robotics Process Automation - New Jersey Business Magazine,” Jun. 11, 2020. https://njbmagazine.com/njb-news-now/7-keys-to-proper-robotics-process-automation/ (accessed Jun. 05, 2022).

[56] van B. Loon, J. Juttmann, H. Chuah, and M. Pouwer, “Adding value through governance, risk management, and controls,” *KPMG*, 2018.

[57] K. L. Murphy, “Robotic Process Automation and Low-Code,” Sep. 19, 2018. https://www.outsystems.com/blog/posts/robotic-process-automation-low-code/ (accessed Jun. 14, 2022).

[58] M. Kelly, “What Is Robotic Process Automation & Why Should Compliance Care

About It? | Risk & Compliance Matters by NAVEX," Jun. 20, 2019. https://www.navexglobal.com/blog/article/what-is-robotic-process-automation-why-should-compliance-care-about-it/ (accessed Jun. 13, 2022).

[59] C. Dilmegani, "What is Robotic Process Automation (RPA)? Ultimate Guide," Nov. 22, 2017. https://research.aimultiple.com/rpa/ (accessed Jun. 14, 2022).

[60] M. Kirchmer, "Robotic Process Automation – Pragmatic Solution or Dangerous Illusion?," Jun. 19, 2017. https://insights.btoes.com/risks-robotic-process-automation-pragmatic-solution-or-dangerous-illusion (accessed Jun. 15, 2022).

[61] A. Jimenez-Ramirez, H. A. Reijers, I. Barba, and C. Del Valle, *A Method to Improve the Early Stages Lifecycle*, vol. 1. Springer International Publishing, 2019.

[62] G. Lawton, "What Is Robotic Process Automation (RPA)? Everything You Need to Know," Apr. 2021. https://www.techtarget.com/searchcio/definition/RPA (accessed Apr. 12, 2022).

[63] L. Willcocks and A. Craig, "Business automation in investment banking: fast forward…. or not? | LSE Business Review," Jan. 27, 2020. https://blogs.lse.ac.uk/businessreview/2020/01/27/business-automation-in-investment-banking-fast-forward-or-not/ (accessed Jun. 17, 2022).

[64] S. Bradford and K. Landrum, "Robotic Process Automation: 4 Key Considerations," Nov. 12, 2019. https://www.informationweek.com/ai-or-machine-learning/robotic-process-automation-4-key-considerations (accessed Jun. 11, 2022).

[65] K. Minolta, "Robotic process automation: when everything runs automatically | KONICA MINOLTA," Jul. 17, 2020. https://www.konicaminolta.eu/eu-en/rethink-work/tools/rpa-what-exactly-is-robotic-process-automation (accessed Jun. 05, 2022).

[66] D. Kedziora and E. Penttinen, "Governance models for robotic process automation: The case of Nordea Bank:," *https://doi.org/10.1177/2043886920937022*, vol. 11, no. 1, pp. 20–29, Jul. 2020, doi: 10.1177/2043886920937022.

[67] R. Todorov, "Approaching Robotic Process Automation with confidence Robotic Process Automation - In a nutshell," p. 14, 2018.

[68] A. Balicki, "Can Robotic Process Automation reduce Operational Risk to zero? | LinkedIn," Jan. 13, 2017. https://www.linkedin.com/pulse/can-robotic-process-automation-reduce-operational-risk-artur-balicki/ (accessed May 27, 2022).

[69] ProV, "Robot Failure: Best Practices for Robotics Process Automation Development," 2021.

[70] Deloitte, "Internal Controls Over Financial Reporting Considerations for Developing

and Implementing Bots," no. September, pp. 1–8, 2018, [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-audit-internal-controls-over-financial-reporting-considerations-for-developing-and-implementing-bots.pdf.

[71] S. Richardson, "Cognitive automation: A new era of knowledge work?," *Bus. Inf. Rev.*, vol. 37, no. 4, pp. 182–189, Dec. 2020, doi: 10.1177/0266382120974601.

[72] S. Pritchard, "How robotic process automation is getting smarter as it evolves," Apr. 12, 2021. https://www.computerweekly.com/feature/How-robotic-process-automation-is-getting-smarter-as-it-evolves (accessed Apr. 28, 2022).

[73] D. Crane, "Contractual considerations in Robotic Process Automation and Artificial Intelligence outsourcing | McCarthy Tétrault," Jul. 25, 2018. https://www.mccarthy.ca/en/insights/blogs/snipits/contractual-considerations-robotic-process-automation-and-artificial-intelligence-outsourcing (accessed Jun. 19, 2022).

[74] S. Matteson, "How Robotic Process Automation can make work more efficient in your business | TechRepublic," Sep. 27, 2021. https://www.techrepublic.com/article/how-robotic-process-automation-can-make-work-more-efficient-in-your-business/ (accessed Apr. 28, 2022).

[75] A. Jiménez-Ramírez, J. Chacón-Montero, T. Wojdynsky, and J. González Enríquez, "Automated testing in robotic process automation projects," *J. Softw. Evol. Process*, 2020, doi: 10.1002/smr.2259.

[76] E. Knutt, "Take out the tedious: robotic automation in government - Global Government Forum," Oct. 14, 2020. https://www.globalgovernmentforum.com/take-out-the-tedious-robotic-automation-in-government/ (accessed Jun. 04, 2022).

[77] BBI, "What is Robotic Process Automation – Benefits and Real-life Cases - Data Driven Digital Transformation | BBI," 2018. https://bbi-consultancy.com/robotic-process-automation-benefits/ (accessed Jun. 05, 2022).

[78] G. Started, "Robotic process automation - understanding the legal issues," 2017.

[79] M. Hunsaker and D. Papenfuss, "Fraud and Emerging Tech: Robotic Process Automation - FEI," Dec. 01, 2020. https://www.financialexecutives.org/FEI-Daily/January-2020/Fraud-and-Emerging-Tech-Robotic-Process-Automatio.aspx (accessed Jun. 11, 2022).

[80] K. Murugappan, T. Sree Kala, T. S. K.-C. S. and D. Forensics, and U. 2022, "An Enhanced Security Framework for Robotic Process Automation," *Springer*, pp. 231–238, 2021, doi: 10.1007/978-981-16-3961-6_20.

[81] A. Jeffs and I. Hawkins, "PEX Guide: What is robotic process automation (RPA)? | Process Excellence Network," Jul. 06, 2021. https://www.processexcellencenetwork.com/rpa-artificial-intelligence/articles/a-guide-to-robotic-process-automation-rpa (accessed Apr. 26, 2022).

[82] Reciprocity, "Compliance Considerations for Robotic Process Automation — Reciprocity," Apr. 19, 2021. https://reciprocity.com/compliance-considerations-for-robotic-process-automation/ (accessed May 04, 2022).

[83] Beroe Inc, "Robotic Process Automation Prone to Cyber Attacks," Jul. 11, 2021. https://www.beroeinc.com/blog/robotic-process-automation-prone-to-cyber-attacks/ (accessed May 15, 2022).

[84] F. Santos, R. Pereira, and J. B. Vasconcelos, "Toward robotic process automation implementation: an end-to-end perspective," *Bus. Process Manag. J.*, vol. 26, no. 2, pp. 405–420, 2020, doi: 10.1108/BPMJ-12-2018-0380.

[85] B. Violino, "6 hidden risks of IT automation," 2020. https://www.cio.com/article/190962/6-hidden-risks-of-it-automation.html.

[86] W. M. P. van der Aalst, M. Bichler, and A. Heinzl, "Robotic Process Automation," *Bus. Inf. Syst. Eng.*, vol. 60, no. 4, pp. 269–272, Aug. 2018, doi: 10.1007/S12599-018-0542-4.

[87] Automation Anywhere, "What is RPA? Robotic Process Automation | Automation Anywhere," 2021. https://www.automationanywhere.com/rpa/robotic-process-automation (accessed May 08, 2022).

[88] AUDITBOARD, "What Is Robotic Process Automation? Can It Assist Internal Audit? | AuditBoard," Jun. 05, 2018. https://www.auditboard.com/blog/5-ways-robotics-process-automation-can-assist-internal-audit/ (accessed Jun. 19, 2022).

[89] G. Gomez, "What is Intelligent Process Automation (IPA)?," Feb. 01, 2020. https://www.bizagi.com/en/blog/intelligent-process-automation/what-is-intelligent-process-automation-ipa (accessed Jun. 14, 2022).

[90] I. Hawkins, "A Guide to Robotic Process Automation (RPA) - iGrafx," Mar. 14, 2019. https://www.igrafx.com/a-guide-to-robotic-process-automation-rpa/ (accessed Jun. 17, 2022).

[91] D. M. West, "How robotic process and intelligent automation are altering government performance," Nov. 16, 2021. https://www.brookings.edu/research/how-robotic-process-and-intelligent-automation-are-altering-government-performance/ (accessed Apr. 26, 2022).

[92] M. Werner, “B Usiness P Rocess a Nalysis a Utomation for F Inancial a Udits,” no. April 2015, pp. 1–9, 2014.

[93] B. Kocsi, M. M. Matonya, L. P. Pusztai, and I. Budai, “Real-time decision-support system for high-mix low-volume production scheduling in industry 4.0,” *Processes*, vol. 8, no. 8, pp. 1–26, 2020, doi: 10.3390/PR8080912.

[94] S. Alexiou, “The Dark Side of Robotic Process Automation,” Aug. 28, 2020. https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/the-dark-side-of-robotic-process-automation (accessed Apr. 28, 2022).

[95] C. Alvarez and N. Salazar, *Robotic Process Automation Risk and Chanllenges - Summer 2020 Prof. Vasarhelyi - YouTube*. YouTube, 2020.

[96] SolveXia, “Everything you Need to Know about Robotic Process Automation,” Apr. 13, 2019. https://www.solvexia.com/blog/everything-to-know-robotic-process-automation (accessed Jun. 11, 2022).

[97] K. C. Moffitt, A. M. Rozario, and M. A. Vasarhelyi, “Robotic Process Automation for Auditing,” *J. Emerg. Technol. Account.*, vol. 15, no. 1, pp. 1–10, Jul. 2018, doi: 10.2308/JETA-10589.

[98] N. Jain, “The risk of RPA implementation and how to mitigate it,” 2020. https://www.capgemini.com/2020/09/the-risk-of-rpa-implementation-and-how-to-mitigate-it/ (accessed Mar. 20, 2022).

[99] K. Gilmurray, “14 rules for Robotic Process Automation (RPA) and Intelligent Automation (AI) success - The AI Journal,” Aug. 06, 2021. https://aijourn.com/14-rules-for-robotic-process-automation-rpa-and-intelligent-automation-ai-success/ (accessed May 08, 2022).

[100] P. Gampe, “Hyper-automation: Hype or help for businesses? | ITProPortal,” Nov. 12, 2021. https://www.itproportal.com/features/hyper-automation-hype-or-help-for-businesses/ (accessed May 15, 2022).

[101] M. Kuppinger, “Robotic Process Automation – an IAM Challenge | KuppingerCole,” May 10, 2019. https://www.kuppingercole.com/blog/kuppinger/robotic-process-automation-an-iam-challenge (accessed Jun. 11, 2022).

[102] N. Bubniuk, “Turbo-Charging Business Operations with Robotic Process Automation - Intellias,” Sep. 30, 2020. https://intellias.com/robotic-process-automation-use-cases/ (accessed Jun. 11, 2022).

[103] S. Wyn and J. Canterbury, “A GAMP® Approach to Robotic Process Automation | Pharmaceutical Engineering,” May 2020. https://ispe.org/pharmaceutical-

engineering/gamp-approach-robotic-process-automation (accessed Jun. 14, 2022).

[104] S. Séguin, H. Tremblay, I. Benkalaï, D.-E. Perron-Chouinard, and X. Lebeuf, "Minimizing the number of robots required for a Robotic Process Automation (RPA) problem," *Procedia Comput. Sci.*, vol. 192, pp. 2689–2698, 2021, doi: 10.1016/J.PROCS.2021.09.039.

[105] J. Spencer, "Beware The Hidden Dangers Of Robotic Process Automation," 2020. https://iig.technology/beware-the-hidden-dangers-of-robotic-process-automation/ (accessed Jun. 13, 2022).

[106] P. Smith, "All you need to know about implementing robotic process automation | ACCA Global," Jun. 2019. https://www.accaglobal.com/ca/en/member/discover/cpd-articles/business-management/rpajun19-cpd.html (accessed Jun. 15, 2022).

[107] I. Limited, "View Point Security Considerations in Robotic Process Automation," 2020.

[108] C. Hutchins, "Robotic Process Automation (RPA): Use Cases And Risks To Consider," 2021. https://www.cioapplications.com/cxoinsights/robotic-process-automation-rpa-use-cases-and-risks-to-consider-nid-4073.html (accessed Jun. 17, 2022).

[109] K. Ng, C. Chen, C. Lee, … J. J.-A. E., and U. 2021, "A systematic literature review on intelligent automation: Aligning concepts from theory, practice, and future perspectives," *Elsevier*, 2021, doi: 10.1016/j.aei.2021.101246.

[110] S. Babic, "Tips for robotic process automation success: Part 2 - The Hyland Blog," Mar. 25, 2021. https://blog.hyland.com/robotic-process-automation/tips-for-robotic-process-automation-success-part-2/ (accessed May 04, 2022).

[111] S. Hanna, "Too many tasks, too little time: Robotic process automation can help | Healthcare IT News," Sep. 30, 2021. https://www.healthcareitnews.com/blog/too-many-tasks-too-little-time-robotic-process-automation-can-help (accessed May 10, 2022).

[112] R. Berg, "Five Robotic Process Automation (RPA) Myths," May 10, 2018. https://content.quanton.co.nz/blog/five-robotic-process-automation-rpa-myths (accessed May 10, 2022).

[113] CiGen, "3 Ways to Settle RPA and Intelligent Automation Fears in Your Organisation – CiGen," Oct. 20, 2020. https://www.cigen.com.au/3-ways-settle-rpa-intelligent-automation-fears/ (accessed Jun. 16, 2022).

[114] J. S. Ågnes, "Gaining and Training a Digital Colleague: Employee Responses to Robotization," *J. Appl. Behav. Sci.*, p. 002188632110435, Sep. 2021, doi:

10.1177/00218863211043596.

[115] M. Dunn, "See why robotic process automation for due diligence has gained momentum and the advantages companies can realize from it. | BIS UK Blog," Mar. 01, 2021. https://bis.lexisnexis.co.uk/blog/categories/governance-risk-and-compliance/automating-due-diligence-RPA (accessed Jun. 08, 2022).

[116] P. Lowes, F. R. S. Cannata, S. Chitre, and J. Barkham, "Automate this: The business leader's guide to robotic process automation," *Deloitte Dev. LLC*, pp. 1–25, 2017, [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-sdt-process-automation.pdf.

[117] S. Goswami, "Robotic Process Automation: Security Essentials," Oct. 17, 2019. https://www.bankinfosecurity.com/interviews/robotic-process-automation-security-issues-i-4480 (accessed Jun. 11, 2022).

[118] R. M. Raiker, "Intelligent Process Mining in Robotic Process Automation | by Ryan M. Raiker, MBA | Towards Data Science," Jul. 19, 2018. https://towardsdatascience.com/intelligent-process-mining-in-robotic-process-automation-f684dd4c7de5 (accessed Jun. 17, 2022).

[119] S. Mitra, "Robotic Process Automation Adoption Challenges & Solutions | EPAM," Jul. 03, 2019. https://www.epam.com/about/newsroom/in-the-news/2019/rpas-adoption-challenges-and-how-to-solve-them (accessed Jun. 08, 2022).

[120] B. Models, "Understanding robotic process automation (RPA)," *Capco Inst. J. Financ. Transform.*, vol. 46, 2017.

[121] J. Chacón-Montero, A. Jiménez-Ramírez, and J. G. Enríquez, "Towards a method for automated testing in robotic process automation projects," *Proc. - 2019 IEEE/ACM 14th Int. Work. Autom. Softw. Test, AST 2019*, pp. 42–47, May 2019, doi: 10.1109/AST.2019.00012.

[122] K. Wiggers, "A definitive primer on robotic process automation | VentureBeat," 2021. https://venturebeat.com/2021/05/02/what-is-robotic-process-automation/ (accessed Apr. 03, 2022).

[123] N. Rashid, "4 Steps To Ensure Robotic Process Automation Security | CDOTrends," Apr. 19, 2021. https://www.cdotrends.com/story/15504/4-steps-ensure-robotic-process-automation-security (accessed May 15, 2022).

[124] C. Tornbohm, "#HowTo: Stay Secure When Deploying Robotic Process Automation - Infosecurity Magazine," 2021. https://www.infosecurity-

magazine.com/opinions/secure-robotic-process-automation/ (accessed Jun. 04, 2022).

[125] CIOReview, "Risk and Control Considerations within an RPA Platform," Jun. 05, 2019. https://www.cioreview.com/news/risk-and-control-considerations-within-an-rpa-platform--nid-29055-cid-75.html (accessed Jun. 11, 2022).

Appendix A

Python code for fetching Google search results

```
#!/usr/bin/env python
# coding: utf-8
# This code fetches google search results in a systematic form for MLR
# Author: António Brites
# Date: November 2021
# Requirements: `pip install request bs4 pandas´

from requests import get
from bs4 import BeautifulSoup
import pandas
import time

def csv_dump(results, name):
    print (results, name)
    df = None
    df = pandas.DataFrame(results)
    df.index += 1
    df.to_csv(name + 'nome.csv')

def parse_results(raw_html):
    soup = BeautifulSoup(raw_html, 'html.parser')
    result_block = soup.find_all('div', attrs={'class': 'g'})
    for result in result_block:
        link = result.find('a', href=True)
        title = result.find('h3')
        if link and title:
            yield { 'URL': link['href'], 'Title': link.text.strip() }

def google_search(query,max_results=500,num_results=100, lang="en"):
    usr_agent ={'User-Agent': 'Mozilla/5.0 (X11; Linuxx86_64; rv:10.0) \ AppleWebKit/537.36 (KHTML, like Gecko)        Chrome/61.0.3163.100 Safari/537.36'}
    escaped_query = query.replace(' ', '+')
    results = []
    for start in range(0,max_results,num_results) :
        google_url = 'https://www.google.com/search?q={}&num={}&start={}&hl={}'.format(escaped_query, num_results+1, start, lang)
        print (google_url)
        time.sleep(3)
        response = get(google_url, headers=usr_agent)
        response.raise_for_status()
        results += parse_results(response.text)
    return results

def get_results(query, name):
    print (query, name)
    results = google_search(query)
    print (results)
    csv_dump(results, name)

if __name__ == '__main__':
    get_results(
        '(Robotic Process Automation OR Intelligent Process Automation) AND Risks', 'risks')

```

Appendix B

Table 5 - List of RPA risks identified by number of mentions over the year

RISKS	2016	2017	2018	2019	2020	2021
ST01 – Misunderstood or missed value	0	1	0	1	1	0
ST02 – Lack of strategic intent	0	0	4	2	3	2
ST03 – Absence of end-point design	0	0	0	1	2	1
ST04 – Isolated/one off goals	0	0	1	2	1	2
ST05 – Under-resourcing your RPA projects	0	1	0	1	0	0
ST06 – Poor strategic reputation	0	1	0	1	0	0
ST07 – Fails to develop a solid business case for RPA	0	0	0	1	0	1
ST08 – General lack of oversight of risk	0	1	3	0	0	0
ST09 – Lack of consistent and secure development and management of bots	0	0	2	0	0	1
ST10 – Poor governance of RPA	0	0	1	3	2	1
SH01 – Employee backlash	0	1	0	1	0	0
SH02 – IT not involved/uncooperative	0	1	0	2	0	0
SH03 – Lack of visible progress and results	0	1	0	1	0	0
SH04 – Poor stakeholder communication	0	0	2	1	0	1
SH05 – Difficulty managing organizational change	0	0	0	1	0	3
SH06 – Lack of experienced RPA resources	0	0	1	1	2	2
SH07 – Difficulty identifying use cases to maintain a healthy automation pipeline	0	1	0	0	0	2
SH08 – Inaccurate analysis	0	0	1	1	0	0
OE01 – Technical issues - Robots stop working or don't function as intended	0	1	4	6	7	1
OE02 – Not enough robots	0	1	0	1	0	0
OE03 – Costly maintenance	1	0	2	2	1	1
OE04 – Not optimising processes before automating them	0	0	1	1	1	4
OE05 – Incorrect process selection	0	1	1	3	1	3
OE06 – Lack of scalability	0	0	0	2	1	2
OE07 – Bad quality of data	0	0	1	2	4	0
OE08 – RPA may hinder real process	0	0	0	1	0	0
OE09 – Lack of standardisation	0	0	0	1	1	0
OE10 – Poor documentation	0	0	1	2	0	0
OE11 – Human error	0	1	1	2	0	1
OE12 – Inefficient implementation of RPA	0	0	4	1	2	0
OE13 – Exception handling	0	0	1	1	3	2
OE14 – Failure to monitor and identify changes to algorithms supporting RPA or the data sources and applications used for automation	0	0	5	2	0	0
OE15 – Senior IT roles may become overburdened	1	0	0	0	0	0
OE16 – Over-automating	0	0	0	0	0	2
OE17 – Reinforcing bias	0	0	0	0	1	0
OE18 – Combine RPA with IA	0	0	0	1	0	1
CM01 – Not building change management capability	0	1	1	1	0	0
CM02 – Human Resources messaging not aligned	0	1	0	2	0	0
CM03 – Unclear roles	0	1	0	1	0	1
CM04 – Lack of user know-how	0	2	3	2	2	5
CM05 – Lack of communication plan	0	1	0	1	3	1
CM06 – Lack of quality and control improvements	1	1	0	1	4	1

CM07 – Lack of formal process for assessing how source application changes affect bots that access them	0	0	2	0	2	2
CM08 – Lack of a formal and consistent process for requesting and implementing changes to bots	0	0	2	1	2	1
CM09 – Lack of segregation of RPA development and production	0	0	2	1	0	0
CM10 – Employee resistance	0	0	1	3	1	0
CM11 – Drive change only by ROI perspective	0	0	1	3	0	0
CM12 – Regulatory risk	0	0	3	1	1	1
CM13 – Failing to Map Dependencies	0	0	0	0	1	1
MT01 – Underutilization of bots	0	1	0	1	0	1
MT02 – Skills leakage/shortage	0	1	2	1	2	2
MT03 – Lack of integration with new technologies	0	1	0	2	3	0
MT04 – General lack of controls	0	0	3	0	0	1
MT05 – Lack of Business continuity preparedness	0	0	1	0	1	0
MT06 – Reputational damage	0	0	0	2	1	0
MT07 – Lack of long-term sustainability	0	0	0	0	1	0
SO01 – Pick wrong advisors/partners or pick right advisors too late	0	3	3	1	1	2
SO02 – Cloud data / compliance risks	0	1	2	4	3	1
SO03 – Fails to determine what IT infrastructure is required to scale and protect the RPA processes	0	0	1	0	0	1
SO04 – Contractual risks	0	0	1	0	0	0
TS01 – Selecting the wrong tool	0	1	3	2	2	0
TS02 – Crowded vendor offerings	0	1	0	2	0	0
TS03 – The ease of getting RPA up and running	0	0	0	1	1	1
LP01 – Unrealistic expectations	0	3	0	2	2	2
LP02 – Try to automate too much	0	1	0	1	0	0
LP03 – Bad shortcuts – testing, documentation, et	0	1	2	3	2	0
LP04 – Underestimating human capital, implementation failure	0	1	0	0	0	1
LP05 – Views RPA as an IT project, not a business initiative	0	0	0	0	0	1
LP06 – Applies traditional software delivery methods to RPA, taking months to deploy when weeks is the norm	0	0	0	0	0	1
LP07 – No component reusability	0	0	0	1	0	0
LP08 – Legacy apps silos	0	0	0	1	3	1
LP09 – Fast implementation	0	0	0	0	2	0
LP10 – Very expensive implementation	1	2	1	2	0	0
LP11 – Risk of redundancy	0	1	0	0	0	0
SC01 – Data leakage	0	0	0	1	2	6
SC02 – Fraud	0	0	1	0	1	5
SC03 – Lack of access management	1	0	2	4	4	4
SC04 – Compromised data	0	0	3	1	4	2
SC05 – Inappropriate access to sensitive data	0	0	2	2	7	0
SC06 – Abuse of administration privileges	0	0	1	0	2	5
SC07 – External threats	0	0	1	3	6	4
SC08 – Internal threats	0	0	0	2	3	1
SC09 – Poor design	0	0	1	3	0	1
SC10 – Unsecure data management	0	0	1	1	5	2
SC11 – Network vulnerability	0	0	3	1	5	4
SC12 – Denial-of-service interruptions	0	0	0	1	1	1
SC13 – Lack of bot accountability relating to security, privacy, and compliance requirements	0	0	3	0	1	1
SC14 – Remote code execution	0	0	0	0	0	0

Appendix C

TABLE 6 - NUMBER OF PUBLICATIONS MENTIONING RISKS

Category Risk	Risks	Mentions as Risks	Total
Strategy Risks	ST01 – Misunderstood or missed value	[38][85][25][37]	4
	ST02 – Lack of strategic intent	[38][85][47][86][54][87][23][43][55][21][88]	11
	ST03 – Absence of end-point design	[38][47][52][21][37]	5
	ST04 – Isolated/one off goals	[38][23][43][22][59][21][37]	7
	ST05 – Under-resourcing your RPA projects	[38][25][37]	3
	ST06 – Poor strategic reputation	[38][25]	2
	ST07 – Fails to develop a solid business case for RPA	[47] [12]	2
	ST08 – General lack of oversight of risk	[56] [70][66][53]	4
	ST09 – Lack of consistent and secure development and management of bots	[56][67][57]	3
	ST10 – Poor governance of RPA	[44][45][22][58][89][49][53]	7
Stakeholders buy-in Risks	SH01 – Employee backlash	[38][25][37]	3
	SH02 – IT not involved/uncooperative	[38][23][25]	3
	SH03 – Lack of visible progress and results	[23][25]	2
	SH04 – Poor stakeholder communication	[85][22][90][53]	4
	SH05 – Difficulty managing organizational change	[47][91][59][90][37]	5
	SH06 – Lack of experienced RPA resources	[47][91][41][92][21][23]	6
	SH07 – Difficulty identifying use cases to maintain a healthy automation pipeline	[47][59][60]	3
	SH08 – Inaccurate analysis	[61][53][93]	3
Operation and Execution Risks	OE01 – Technical issues - Robots stop working or don’t function as intended	[38][85][48][9][62][39][41][94][44][45][68][95][96][70][97][63][49][12][53][98]	20
	OE02 – Not enough robots	[38][25]	2
	OE03 – Costly maintenance	[38][39][35][64][59][70][53]	7
	OE04 – Not optimising processes before automating them	[85][74][99][100][22][49][53]	7
	OE05 – Incorrect process selection	[48][72][95][22][96][59][90][13][53]	9
	OE06 – Lack of scalability	[62][74][23][101][102]	5
	OE07 – Bad quality of data	[23][65][103][89][52][12][53]	7
	OE08 – RPA may hinder real process	[23]	1
	OE09 – Lack of standardisation and no component reusability	[23][66]	2
	OE10 – Poor documentation	[23][67][49]	3
	OE11 – Human error	[23][68][67][58][104]	5
	OE12 – Inefficient implementation of RPA	[44][67][105][106][70][97][53][37]	8
	OE13 – Exception handling	[66][69][67][107][103][108][49][37]	8
	OE14 – Failure to monitor and identify changes to algorithms supporting RPA or the data sources and applications used for automation	[23][43][45][67][70][97][53]	7
	OE15 – Senior IT roles may become overburdened	[35]	1
	OE16 – Over-automating	[58][104]	2
	OE17 – Reinforcing bias	[71]	1
	OE18 – Combine RPA with IA	[12][109]	2
Change Management Risks	CM01 – Not building change management capability	[38][25][53]	3
	CM02 – Human Resources messaging not aligned	[38][23][25]	3
	CM03 – Unclear roles	[38][72][25][37]	4
	CM04 – Lack of user know-how	[38][25][26][91][110][87][23][111][112][19][113][13][114][53]	14
	CM05 – Lack of communication plan	[38][25][87][95][113][63][37]	7
	CM06 – Lack of quality and control improvements	[25][34][91][94][45][55][21][63]	8
	CM07 – Lack of formal process for assessing how source application changes affect bots that access them	[18][66][59][52][57][53]	6
	CM08 – Lack of a formal and consistent process for requesting and implementing changes to bots	[56][44][103][59][70][12][37]	7
	CM09 – Lack of segregation of RPA development and production	[56][23][53]	3
	CM10 – Employee resistance to change	[23][113][90][70][12]	5
	CM11 – Drive change only by ROI perspective	[23][112][90][12]	4
	CM12 – Regulatory risk	[115][21][70][73][49][53]	6
	CM13 – Failing to Map Dependencies	[22][105]	2
	MT01 – Underutilization of bots	[38][69][25]	3
	MT02 – Skills leakage/shortage	[38][25][47][56][91][21][71][53]	8

Maturity Risks	MT03 – Lack of integration with new technologies	[38][23][66][105][21][25][37]	7
	MT04 – General lack of controls	[56][57][63][53]	4
	MT05 – Lack of Business continuity preparedness	[44][97][37]	3
	MT06 – Reputational damage	[44][45][49]	3
	MT07 – Lack of long-term sustainability	[52][37]	2
Sourcing Risks	SO01 – Pick wrong advisors/partners or pick right advisors too late	[38][25][116][39][99][112][59][60][73] [53]	10
	SO02 – Cloud data / compliance risks	[38][25][44][100][55][117][58][103][118][49] [53]	11
	SO03 – Fails to determine what IT infrastructure is required to scale and protect the RPA processes	[47][70]	2
	SO04 – Contractual risks	[73]	1
Tool Selection Risks	TS01 – Selecting the wrong tool	[38][25][91][39][41][94][49][53]	8
	TS02 – Crowded vendor offerings	[38][25][49]	3
	TS03 – The ease of getting RPA up and running	[47][41][12]	3
Launch / Project Risks	LP01 – Unrealistic expectations	[38][25][47][99][119][120][52][60][21]	9
	LP02 – Try to automate too much	[38][25]	2
	LP03 – Bad shortcuts – testing, documentation, etc	[38][25][23][73][14][75][121][53]	8
	LP04 – Underestimating human capital, implementation failure	[25][47]	2
	LP05 – Views RPA as an IT project, not a business initiative	[47]	1
	LP06 – Applies traditional software delivery methods to RPA, taking months to deploy when weeks is the norm	[47]	1
	LP07 – No component reusability	[23]	1
	LP08 – Legacy apps silos	[23][105][103][59][21]	5
	LP09 – Fast implementation	[76][52]	2
	LP10 – Very expensive implementation	[35][51][77][64][120][49]	6
	LP11 – Risk of redundancy	[78]	1
Security Risks	SC01 – Data leakage	[40][48][122][123][83][124][21][80][14]	9
	SC02 – Fraud	[40][47][123][43][124][79][80]	7
	SC03 – Lack of access management	[122][91][41][42][23][35][67][125][101][117] [107][103][21][70][80]	15
	SC04 – Compromised data	[62][91][39][43][95][107][90][97][63][53]	10
	SC05 – Inappropriate access to sensitive data	[47][39][81][56][82][42][83][95][107] [90][80]	11
	SC06 – Abuse of administration privileges	[47][39][81][82][42][21][80][53]	8
	SC07 – External threats	[53][81][41][83][95][124][55][107][90][21] [97][49][79][14]	14
	SC08 – Internal threats	[53][44][124][14][90][21]	6
	SC09 – Poor design	[53][42][117][49][70]	5
	SC10 – Unsecure data management	[53][41][42][44][107][21][97][63][79]	9
	SC11 – Network vulnerability	[53][39][110][42][54][44][95][124][103] [21][97][73][80]	13
	SC12 – Denial-of-service interruptions	[53][39][80]	3
	SC13 – Lack of bot accountability relating to security, privacy, and compliance requirements	[53][56][103][97][80]	5
	SC14 – Remote code execution	[83]	1