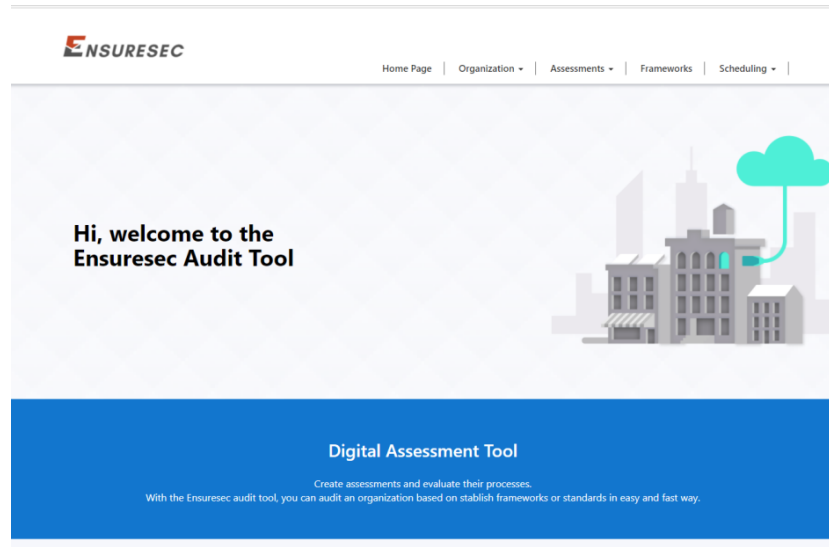




**TÉCNICO**  
LISBOA



# **Using a Software Tool for Assessing the Maturity Level of Good Management Practices**

**Alexandre Manuel Ferreira do Amaral**

Thesis to obtain the Master of Science Degree in  
**Information and Enterprise Systems**

Supervisors: Prof. Miguel Leitão Bignolas Mira da Silva  
Prof. Rúben Filipe de Sousa Pereira

## **Examination Committee**

Chairperson: Prof. Daniel Jorge Viegas Gonçalves  
Supervisor: Prof. Miguel Leitão Bignolas Mira da Silva  
Member of the Committee: Prof. Isabel Maria Mendes Pedrosa

**November 2021**



# Acknowledgments

While performing this thesis I received constant support and help from different persons.

I would like to thank my supervisors, Professor Miguel Mira da Silva and Professor Ruben Pereira and the PhD student André Fernandes whose expertise was invaluable in guiding me on having the best results possible on this investigation.

Also, I would like to thank all the auditors that were part of this investigation.

Finally, related to my personal life, I would like to acknowledge my girlfriend for encouraging me in doing this master degree. I will be forever grateful to her.



# Resumo

As organizações usam frequentemente frameworks reconhecidas internacionalmente para verificar a capacidade e resiliência dos seus processos. Estas frameworks permitem às organizações posicionarem-se melhor face aos concorrentes através da melhoria dos seus processos, definindo objetivos e encontrando soluções para os problemas detetados. No entanto, as avaliações destes processos são geralmente morosas e pouco organizadas, tornando-as dispendiosas para as empresas.

Este trabalho de investigação propõe a criação e implementação de uma ferramenta de software que permite aos auditores determinar, de uma forma precisa e eficiente, a capacidade de um processo dentro de uma organização. Esta investigação foi suportada pela metodologia *Design Science Research*, que permitiu desenhar e desenvolver um artefacto; demonstrar a sua utilidade; e avaliar se este pode ser utilizado para solucionar o problema identificado.

No decorrer desta investigação, a equipa desenvolveu o modelo da ferramenta, que foi depois instanciado na forma de uma aplicação web. A ferramenta foi posteriormente melhorada com base no feedback recolhido em duas fases distintas: em duas entrevistas com auditores experientes; e durante um estudo realizado com um estudante de mestrado.

Os resultados sugerem que a utilização da ferramenta parece melhorar o trabalho do auditor, ao suportar as suas atividades. No entanto, o artefacto proposto ainda está numa fase bastante inicial, precisando de diversas melhorias antes de poder ser utilizado num contexto real.

No futuro, as sugestões de melhoria serão implementadas, nomeadamente o suporte de normas que não sigam a estrutura da família de standards ISO/IEC 330xx, a qual não parece ser usada na indústria.

**Palavras-Chave:** Auditoria, Ferramenta de Auditoria, Frameworks de Capacidade, Modelo de Maturidade, Norma Internacional.



# Abstract

Organizations often use recognized frameworks to assess the capability of their processes. These frameworks allow organizations to better position themselves, define goals, and find solutions to achieve those goals. However, the evaluation process is often time-consuming, poorly organized, and expensive for the organizations that hire the audit services themselves.

To address this problem, we propose to implement a software tool to help assessors in determining the capability of a process concisely and efficiently. This research follows a Design Science Research methodology to design and develop this artefact, to demonstrate its usefulness, and to evaluate if and how it can be used to address the stated problem.

We developed a model for the software tool, which was instantiated as a PowerApps web application. The tool was later improved based on the feedback received during two interviews with experienced auditors and a field study with a master student. The improved version was evaluated with a set of interviews with eight experienced auditors.

Overall, supporting an audit process with a software tool seems to improve the auditor on its work, but the proposed artefact is still in a very initial stage, and many improvements are needed before it can be used in a real organization. In the future, the improvements suggested should be implemented, particularly the support for standards that do not follow the structure of the ISO/IEC 330xx family of standard, which does not seem to be used in the industry.

**Keywords:** Assessment, Assessment Tool, Capability Frameworks, Maturity Model, International Standard.





# Table of Contents

- Acknowledgments .....iii**
- Resumo .....v**
- Abstract.....vii**
- Table of Contents.....ix**
- List of Figures .....xi**
- List of Tables.....xiii**
- List of Acronyms.....xv**
- 1. Introduction .....1**
  - 1.1. Document Outline .....2
- 2. Research Problem .....3**
  - 2.1. Interviews .....3
  - 2.2. Problem Statement .....7
- 3. Research Methodology .....9**
  - 3.1. Systematic Literature Review .....9
  - 3.2. Design Science Research .....9
- 4. Research Background.....13**
  - 4.1. ISO/IEC 330xx.....13
  - 4.2. Commercial Tools .....15
- 5. Literature Review.....17**
  - 5.1. Planning .....17
    - 5.1.1. Research Questions .....17
    - 5.1.2. Search Process .....17
    - 5.1.3. Inclusion and Exclusion Criteria .....18
    - 5.1.4. Data Extraction and Synthesis .....19
  - 5.2. Conducting .....20
  - 5.3. Reporting.....25
    - 5.3.1. Does the use of a software tool to support the audit processes can help assessors' organizing and optimizing their work? .....25
    - 5.3.2. Which tools already exist to support audit processes? .....25
- 6. Proposal.....27**

6.1. Objectives.....	27
6.2. Description .....	27
<b>7. Demonstration .....</b>	<b>35</b>
7.1. Tool Prototype.....	35
7.1.1. Framework Loading.....	41
7.2. Improved Tool.....	43
7.2.1. Automatic Process Rate .....	43
7.2.2. Reporting .....	45
7.2.3. Other improvements .....	45
<b>8. Evaluation.....</b>	<b>49</b>
8.1. Interviews for Tool Validation .....	49
8.2. Field Study .....	50
8.3. Final Interviews with Experts.....	50
8.4. Discussion .....	53
<b>9. Conclusion.....</b>	<b>55</b>
9.1. Lessons Learned .....	56
9.2. Contributions .....	56
9.3. Limitations .....	57
9.4. Future Work.....	57
<b>Bibliography.....</b>	<b>59</b>

# List of Figures

<b>Figure 3.1.</b> DSR methodology process model (adapted from [10]) .....	10
<b>Figure 3.2.</b> Dissertation chapters where the different DSR phases are described .....	10
<b>Figure 4.1.</b> Assessment structure proposed by the ISO/IEC 33052 and ISO/IEC TS 33072 standards .....	14
<b>Figure 6.1.</b> Paper selection process.....	20
<b>Figure 6.2.</b> Technologies used in the selected papers .....	21
<b>Figure 6.3.</b> Most common functionalities .....	23
<b>Figure 6.4.</b> Research methods applied in the selected papers .....	24
<b>Figure 7.1.</b> UML diagram of the software tool.....	30
<b>Figure 7.2.</b> Create Organization – Functionality Activity Diagram .....	30
<b>Figure 7.3.</b> Meeting scheduling – Functionality Activity Diagram.....	31
<b>Figure 7.4.</b> Create new assessment – Functionality Activity Diagram .....	31
<b>Figure 7.5.</b> Add evidence to an outcome – Functionality Activity Diagram.....	32
<b>Figure 7.6.</b> Evaluate process based on evidence – Functionality Activity Diagram.....	32
<b>Figure 7.7.</b> Evaluate outcomes based on evidence – Functionality Activity Diagram.....	33
<b>Figure 7.8.</b> Insert frameworks individually, using the front end – Functionality Activity Diagram .....	34
<b>Figure 7.9.</b> Insert frameworks in bulk, using the backoffice – Functionality Activity Diagram .....	34
<b>Figure 8.1.</b> Login page of the application .....	35
<b>Figure 8.2.</b> Homepage of the application .....	36
<b>Figure 8.3.</b> List of organizations.....	36
<b>Figure 8.4.</b> Page for creating an organization .....	37
<b>Figure 8.5.</b> List of meetings scheduled.....	37
<b>Figure 8.6.</b> Create a schedule for a meeting. ....	38
<b>Figure 8.7.</b> List of assessments .....	38
<b>Figure 8.8.</b> Edit assessment page .....	39
<b>Figure 8.9.</b> Edit a process associated to an assessment.....	40
<b>Figure 8.10.</b> Edit the outcome of a process that is associated to an assessment.....	40
<b>Figure 8.11.</b> PowerApps backoffice where the table <i>Process</i> is accessed, with the “Edit data in Excel” option highlighted with a red rectangle.....	41

**Figure 8.12.** Excel file containing the information for the *Process* table of the application database...42

**Figure 8.13.** List of frameworks added in the application using the insert in bulk functionality .....42

**Figure 8.14.** Page for inserting a framework using the front-end.....43

**Figure 8.15.** Flow for automatically setting the rate of a process when all outcomes are rated as “Partially achieved” or “Largely achieved”. .....44

**Figure 8.16.** Assessment page, from where the auditor can access the assessment report by clicking on “Final Report” button (highlighted with a red rectangle).....46

**Figure 8.17.** Assessment report. The auditor can print it by clicking on the “Print” button (highlighted with a red rectangle).....46

**Figure 8.18.** Report on the tool .....47

**Figure 8.19.** Form for creating an organization, with the new Address field (highlighted with a red rectangle).....47

**Figure 8.20.** Navigation bar on the assessments page improved (highlighted with a red rectangle) ...48

# List of Tables

<b>Table 2.1.</b> Interview Guide .....	3
<b>Table 2.2.</b> Interviewees' profile .....	4
<b>Table 2.3.</b> Frameworks that the interviewees work with. ....	5
<b>Table 2.4.</b> Tasks performed to prepare an audit.....	5
<b>Table 2.5.</b> Challenges that can have a negative impact on audits .....	6
<b>Table 2.6.</b> Functionalities suggested by the interviewees for a software tool .....	7
<b>Table 4.1.</b> Compliance Software Tools investigated .....	16
<b>Table 5.1.</b> Studies included in the SLR.....	21
<b>Table 5.2.</b> Stakeholders in focus in selected papers .....	22
<b>Table 5.3.</b> Frameworks and maturity models supported by the tools studied in selected papers.....	22
<b>Table 5.4.</b> Functionalities .....	23
<b>Table 5.5.</b> Target challenges considered in the selected studies .....	24
<b>Table 5.6.</b> Results observed in the selected studies. Greyed rows correspond to positive results.....	24
<b>Table 5.7.</b> Summary of the identified tools' characteristics. ....	25
<b>Table 6.1.</b> Tasks performed by the auditors and functionalities proposed for a software tool, mentioned in each research method.....	28
<b>Table 6.2.</b> Tool requirements. ....	29
<b>Table 7.1.</b> Requirements for the reporting functionality .....	45
<b>Table 8.1.</b> Bugs reported during the field study.....	51
<b>Table 8.2.</b> Improvements suggested by the interviewees.....	52



# List of Acronyms

<b>CMMI</b>	Capability Maturity Model Integration
<b>DSR</b>	Design Science Research
<b>ISO</b>	International Standardization Organization
<b>ITIL</b>	Information Technology Infrastructure Library
<b>PAM</b>	Process Asssesment Model
<b>PRM</b>	Process Reference Model
<b>SLR</b>	Systematic Literature Review
<b>COBIT</b>	Control Objectives for Information and Related Technologies
<b>NIST</b>	National Institute of Standards and Technology
<b>IDI</b>	INTOSAI Development Initiative
<b>GDPR</b>	General Data Protection Regulation)
<b>NERC CIP</b>	North American Eletric Reliability Corportation Critical Infrastructure Protection
<b>PCI DSS</b>	Payment Card Industry Data Security Standard
<b>CSA</b>	Canadian Standards Association





# 1. Introduction

Aiming at delivering products and services while respecting quality, time, and budget requirements, many organizations have been applying well-known and defined frameworks to assess the capability of their organizational processes [1].

Some popular examples of internationally accepted frameworks include maturity models such as Capability Maturity Model Integration (CMMI) [2] and Information Technology Infrastructure Library (ITIL) [3], and international norms such as those published by the International Standardization Organization (ISO) [4], from which ISO 27001 [5] and ISO 9001 [6] are popular examples.

The application of these frameworks can widely help organizations improving their operational effectiveness and efficiency. By defining better goals and finding solutions to achieve those goals, organizations can achieve a mindset of continuous improvement and innovation [7]. Moreover, a certification on an international standard act as a recognition of the organization's commitment to the best practices in the industry. This allows the organization to better position themselves [8] and can be a competitive advantage to attract new clients.

The process assessment, or audits, are used to examine the compliance between the organizational processes and the frameworks. They generate results that organizations can use to analyze their current practices; identify areas for improvement and plan the steps towards those improvements [9]. By comparing the current state of the processes against a set of defined goals (which can be defined by the organization or can be requirements established in a framework), process gaps can be identified and addressed.

Audits are usually conducted by expert assessors (either internal or external to the organization), often using traditional collaboration tools, such as e-mail or physical documents, to collect evidence; rate process capabilities; and write assessment reports. However, the fact that these activities are very complex; time-consuming; and often supported by outdated tools, makes the audit process expensive, preventing organizations from running these audits [10].

To address this problem, we propose the use of a software tool to assist assessors in conducting audits and determining the capability of a process. With this solution, we intend to provide more support for auditors to perform their work and organize the audit process, thus improving the efficiency and effectiveness of those processes, while reducing associated costs.

This research was conducted by following a Design Science Research (DSR) methodology, which allowed us to design, develop, test, and evaluate an artefact that can be proven to be effective in real-world scenarios [11].

We started by conducting an in-depth analysis to establish the problem and the goals for a solution, based on a set of interviews with experienced auditors; an analysis of commercial compliance software tools; and a systematic literature review on the topic.

The results of this in-depth analysis were then used to build a model for a software tool, comprising the functionalities that seemed to be more useful to the auditors to improve the audit process efficiency, based on the previous research activities. This model was later instantiated as a web application. After loading two different frameworks into the tool, we validated it by conducting two interviews with experienced auditors and a field study with a master student.

The feedback received during these validation interviews was used to improve the tool, by addressing minor improvements and implementing two new functionalities. The improved tool was evaluated during a set of interviews with the same experienced auditors that participated in the problem definition. The outputs of this evaluation activity were important to understand if the proposal can be used to address the research problem and achieve the defined goals.

Overall, we found that supporting an audit process with a software tool can assist the auditor on its work, but it is still in a very initial stage, and many improvements are needed before it can be used in a real organization.

This research work was done under the scope of the H2020 ENSURESEC project<sup>1</sup>, funded by the European Union under grant agreement number 883242.

## 1.1. Document Outline

The structure of this document is highly influenced by the methodology used to conduct this research, which is further discussed in Section 3.2.

In Chapter 2, we start by describing the research problem and motivation for this work. In Chapter 3 we describe the research methodology followed, which included a Systematic Literature Review (SLR).

After presenting the research background underlying this work in Chapter 4, we describe the SLR conducted to understand the impact of software tools in the audit process in Chapter 5.

In Chapter 6 we explain in detail our research proposal, which consists on a model composed by a set of functionalities; its requirements; an UML diagram; and an activity diagram for each functionality. Then, in Chapter 7 how the proposal was demonstrated by developing and populating a functional prototype, and the evaluation activities are described in Chapter 8. Finally, in Chapter 9 we present our conclusions; contributions; research limitations; and future work.

---

<sup>1</sup> Ensuresec project: <https://www.ensuresec.eu/> (Accessed 29/08/2021)

# 2. Research Problem

Audits are a very bureaucratic process often conducted with manual procedures and outdated tools, which represent many challenges for both assessors and organizations. During audits, a large amount of evidence must be collected from multiple sources, which can difficult the analysis of the outputs [12], and makes it harder to achieve an objective evaluation [13].

Additionally, the reliability and precision of the data collected can be compromised [14], particularly due to the bias caused by the participants and assessor’s attitudes, experience, and approach, which are often subjective [3]. This issue is amplified by the lack of transparency in the way audits are conducted, where relevant information regarding the process is not visible [15]. All this leads to audits that are inefficient, time-consuming, and expensive to the organizations [16], [17].

## 2.1. Interviews

To identify the specific challenges underlying the audit processes, and thus improve the understanding of the research problem, we conducted semi-structured interviews with experienced auditors. The objective was to gather feedback about the problems that can happen during audit processes and to understand some aspects of the organizations that hire this type of services.

The interview guide is presented in Table 2.1 and was organized in three sections: warm-up (to know the profile of the interviewee); audits (to understand their experience and opinion regarding audit processes); and final remarks.

**Table 2.1.** Interview Guide

<p><b>Warm-up</b></p> <ul style="list-style-type: none"><li>– Briefly describe your career path.</li><li>– Briefly describe your academic background.</li><li>– Can you describe your main responsibilities and tasks as an auditor?</li><li>– Which frameworks do you usually work with?</li></ul>
<p><b>Audit Process</b></p> <ul style="list-style-type: none"><li>– Which tasks do you usually perform to prepare an audit?</li><li>– In your opinion, how can the organization that is being audited can be involved in the process to facilitate the auditor’s work?</li><li>– Based on your experience, which challenges usually have a negative impact on an audit process? From those, which ones have the highest and the lowest impact?<ul style="list-style-type: none"><li>• Do you think that organizations usually audit their processes? If yes, which do you think that are their motivations? If no, why do you think this happens?</li></ul></li><li>– Based on your experience, which are the usual characteristics of the organizations that conduct audits (E.g. size)</li><li>– Do you believe that using a software to support the main tasks would improve the audit processes? How?</li></ul>
<p><b>Final remarks</b></p> <ul style="list-style-type: none"><li>– Regarding the topics discussed, is there any other relevant information you want to share with us?</li></ul>

The interviews were held remotely (via Zoom) between January 2021 and March 2021 and took between 30 minutes and one hour. The interviews were recorded (with the permission of the interviewees) and then revised to take notes and organize the results. The participants were selected based on the contacts of the researchers and on LinkedIn (by searching for auditors).

Eight Portuguese auditors (including four lead auditors) were interviewed, and their profile can be found on Table 2.2. Most interviewees have a computer science background, but their professional experience is more varied. A1 and A2 are the most experienced auditors, with 31 and 23 years of experience, respectively, as auditors and project managers. A6 is the less experienced one, with two years of professional experience as an auditor. The remaining have between six and 10 years of professional experience.

Moreover, these interviewees currently work in different sectors, including Energy (N=3); Consulting (N=2); Finance (N=1); Banking (N=1); and Telecom (N=1).

**Table 2.2.** Interviewees' profile

ID	Role	Business Sector	Academic Background	Professional Experience	Years of Experience
A1	Lead Auditor	Consulting	Information Systems Management	Project Manager Auditor	31
A2	Lead Auditor	Consulting	Applied Maths	Quality Manager Project Manager Auditor	23
A3	Auditor	Finance	Computer science	Researcher Startup Founder Auditor in Finance	8
A4	Auditor	Energy	Computer science	Senior Advisor in Information Risk Management IT Auditor	6
A5	Lead auditor	Energy	Computer science	IT Compliance and Risk Manager Lead Auditor	10
A6	Auditor	Telecom	Computer science	IT Asset Manager IT auditor	2
A7	Lead Auditor	Energy	Information Systems and Computer Engineering	IT Advisor Internal auditor	8
A8	Auditor	Banking	Microeletronics and Nanotechnologies Engineering	Information Systems Auditor	6

In Table 2.3 we show the standards that each auditor works within his organization. Except for A2, all auditors work with the ISO 27001 norm, which is related to Information Security. Furthermore, A1 also works with other norms from the ISO 27xxx family. Likewise, COBIT was mentioned by all auditors but A2. Half the interviewees also work with ITIL, and three of them work with the ISO 20000 norm (A1, A2, and A8). Also related to security, the NIST cybersecurity framework was mentioned by three auditors.

The tasks that auditors more often perform to prepare an audit are shown in Table 2.4.

**Table 2.3.** Frameworks that the interviewees work with.

Framework		A1	A2	A3	A4	A5	A6	A7	A8
ISO 27xxx Family	ISO 27001	X		X	X	X	X	X	X
	ISO 27017	X							
	ISO 27018	X							
	ISO 27701	X							
COBIT		X		X	X	X	X	X	X
ITIL		X			X		X	X	
ISO 20xxx Family	ISO 20000	X	X						X
	ISO 20001		X						
NIST					X	X		X	
ISO 22301		X							
ISO 9001			X						
IDI			X						
Ticket			X						
CMMI			X						
GDPR				X					
NERC CIP					X				
PCI DSS						X			
CSA						X			
ISO 3100								X	

**Table 2.4.** Tasks performed to prepare an audit

	A1	A2	A3	A4	A5	A6	A7	A8
Define stakeholders for each process that will be audited	X	X		X	X		X	X
Create audit plan	X		X	X				X
Collect information about the organization	X	X						
Assign responsible for managing the communication between auditors and employees	X	X						
Notify departments that will be audited					X	X		
Determine the people responsible by each requirement of the framework		X						
Determine the departments affected by the audit		X						
Ensure the audit plan is approved by top management				X				
Create test plans							X	
Consult results of previous audits for the audited frameworks and processes							X	

We found that the tasks performed to prepare an audit differ with the interviewees profile. For example, the two auditors that perform consultancy work in different organizations, A1 and A2, mentioned the need to know more about the organization that will be audited, mainly because it is important for them to understand how the organization operates in the market and how it is organized. Additionally, they also mentioned the need to assign a responsible for managing the communication between the auditors and employees.

Nevertheless, there are tasks that are commonly mentioned by either internal or external auditors, such as the need to prepare an audit plan and the definition of relevant stakeholders for each process that will be audited.

Regarding how organizations can help the auditors perform their work, the interviewees overall stated that their work would improve if the organization defined the relevant stakeholders that are supposed to be participating in the audit process. Also, A1 and A2 stated that an audit process is usually faster when the organization ensures that the relevant information is well organized and structured, so that the auditor can better understand it.

On the other hand, there are some common challenges affecting audits, which are listed in Table 2.5. Some auditees can try to mislead the auditor with false information about the processes that are being audited, to influence the results. Having unorganized information can also negatively impact an audit process. Finally, another common issue is the stress of the employees being audited.

**Table 2.5.** Challenges that can have a negative impact on audits

	A1	A2	A3	A4	A5	A6	A7	A8
False information given when auditing the processes	X	X			X	X	X	X
Unorganized information	X	X	X		X		X	
Employees being audit get stressed	X	X			X			
Lack of maturity of the organization			X					
Unclear management expectations on what will be audited or not				X				

Concerning the characteristics and motivations of the organizations being audited, all auditors agreed that, in the Portuguese context, organizations only conduct audits by need. These organizations are often big companies that are regulated by laws or that depend heavily of their reputation in the market. However, their characteristics are widely dependent on their area of operation.

Finally, all auditors agreed that having a software to support audit processes could help them on making assessment. They also pointed out some functionalities that could be included in such a tool, which are displayed on Table 2.6.

**Table 2.6.** Functionalities suggested by the interviewees for a software tool

	A1	A2	A3	A4	A5	A6	A7	A8
Report generation	X	X	X		X	X		
Evidences management	X		X	X		X	X	
Forms to gather information	X			X				
Meeting scheduling		X			X			
Continuous Improvement					X		X	
Set responsible by process		X						
Alerts			X					

The two most mentioned functionalities were the possibility to generate reports and support for evidences management. The latter consists on managing the evidences collected during the audit, so that all evidences that support a requirement of the standard can be easily found, for example.

Two auditors further suggested to have a functionality for the auditors to create forms to collect information outside audit meetings. Other two auditors further suggested that such an application would support an agenda functionality to schedule meetings for an audit, and two suggested support for continuous improvement (i.e. connect different audits, so that the results of an audit can be considered in a following one).

## 2.2. Problem Statement

Overall, we found that auditors work with a wide range of different frameworks, and perform different tasks to prepare for an audit, depending on their profile. Nevertheless, most of the auditors interviewed prepare an audit by creating an audit plan and defining stakeholders for each process that will be audited, which can be easily done with the help of the organization. Moreover, the audit process can be faster if the organization ensures that the relevant information is organized and structured.

We identified some challenges that audit processes may be subject to, namely regarding the employees being stressed and providing false information when their work is being audited. Having information unorganized and non-visible during the audit process can also lead to a lack of transparency.

Finally, there seems to be benefit in having a software tool to support audit processes, which could help addressing some of the challenges and supporting preparation tasks.

Summing up, the problem we are addressing in this research work is the **lack of a structured, transparent, and efficient approach to collect and evaluate evidence during audits.**





# 3. Research Methodology

In this Chapter we explain the research methodologies that will be followed to address the identified problem: systematic literature review (SLR) and DSR approach.

## 3.1. Systematic Literature Review

A SLR was conducted by following the original guidelines proposed by Kitchenham and Charters for performing SLRs in software engineering [18], which define that an SLR method comprises three consecutive stages:

- **Planning:** including the identification of the need for a review; specification of research questions; and development of the review protocol;
- **Conducting:** including the identification of research; selection of primary studies; data extraction and monitoring; and data synthesis.
- **Reporting:** including the writing of the report; and dissemination of results.

This SLR was managed and documented using Parsifal<sup>2</sup>, an open-source web application based on the steps suggested by Kitchenham and Charters [19]. The knowledge produced by applying this methodology (which will not be further described in this document) will help defining the steps of the DSR methodology.

## 3.2. Design Science Research

This research followed a DSR approach, which is focused on creating and evaluating new and innovative artefacts (such as constructs, models, methods, and instantiations [20]) that are intended to solve organizational problems concerning both IT and organizations [21]. These artefacts and their implementation processes are based on existent knowledge. In turn, their evaluation generates new knowledge that can be used by practitioners to design solutions for their field problems, and so on [22].

In DSR there is a clear alignment between the cycles of design, relevance and rigour (described by Hevner et al. [23]) that link the research context to the DSR activities, and these to the existent knowledge. This link reveals the importance of the DSR paradigm for research in information systems, which is increasingly gaining general acceptance as a legitimate research methodology [24].

DSR is guided by a set of conceptual principles, practices (in the form of seven guidelines proposed by Hevner et al. [23]) and an iterative process composed by six phases [11]:

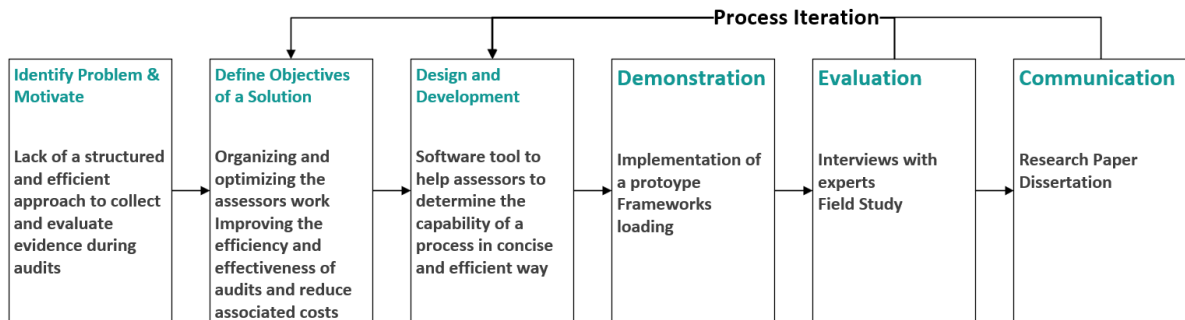
- **Problem identification and motivation:** identify and define the research problem and justify the value of a solution.

---

<sup>2</sup> Parsifal: <https://parsif.al> (Accessed 13/10/2021)

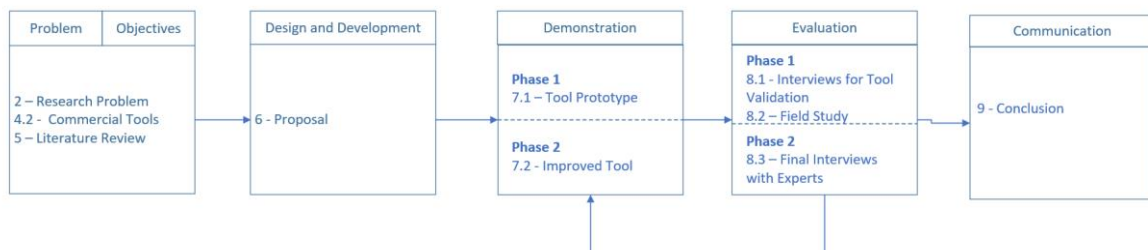
- **Define the objectives for a solution:** identify the objectives for the solution, based on the problem definition and knowledge of the state of the art and possible solutions.
- **Design and development:** Determine the artefact's desired functionality and architecture, and then create the actual artefact. An artefact can be any created object with the research contribution embedded in the design.
- **Demonstration:** demonstrate the use of the artefact to solve one or more cases of the problem.
- **Evaluation:** observe and measure how well the artefact supports a solution to the problem. This involves comparing the objectives of the solution to the results observed from using the artefact in the demonstration.
- **Communication:** communicate the problem and its importance; the artefact; its utility and novelty, the rigor of its design and its effectiveness to researchers and other relevant audiences.

This process model is presented in Figure 3.1, applied to our research work.



**Figure 3.1.** DSR methodology process model (adapted from [11])

Therefore, by using DSR we were able to design, develop, test, and evaluate an artefact that can be proven to be effective in real-world scenarios [11]. While we only had the opportunity to conduct one iteration, we were able to perform minor improvements on the proposed artifact, thus the activities of the Demonstration and Evaluation phases were performed in two phases. The diagram in Figure 3.2 maps the different DSR phases to the chapters in this dissertation where they are described.



**Figure 3.2.** Dissertation chapters where the different DSR phases are described

The first step was identifying and defining the problem that motivated the research, followed by the definition of the objectives for the solution. These activities were supported by the results of a set of

interviews with experts; an analysis of commercial tools available to support audit processes; and a SLR on the topic.

Based on the result of these activities, we created a model for that solution that could help achieve those objectives and address the research problem. This model was then instantiated as a web app, and two frameworks were loaded to demonstrate that the tool was generic enough to support different frameworks.

This original tool was then evaluated based on two interviews and a field study, which provided inputs for implementing some improvements in a second phase. In turn, the improved tool was evaluated based on a set of interviews with the same experts that participated in the problem definition and objectives identification. Overall, this allowed us to evaluate the quality of the model and its instantiation to address the research problem.

Based on the results collected, we derived important conclusions and lessons learned, and communicated those results to the relevant audiences.



# 4. Research Background

To achieve operational efficiency, organizations must guarantee that their processes are efficient and align with their business objectives. This can be accomplished by evaluating those processes against a set of defined target goals, which translate the desired process status. With this, organizations can identify gaps, and suggest and implement improvements.

These evaluations are often based on the reported results of audits, which are conducted by auditors (either an individual or a group of people) on specific processes [25]. While the audit is being held, the main role of the auditor(s) is to gather the information related to the processes that are being audited, using different techniques such as interviews or document analysis. Then, the processes are evaluated against that previously defined set of goals [26].

On the other hand, these goals can be derived from diversified sources. For example, senior management can establish a business goal that requires changes in one or more of the already existent processes. Additionally, the organization can decide to align their practices with the requirements established by a recognized framework, since it allows them to better position themselves; define goals; and find solutions based on globally accepted requirements.

An example of such frameworks are standard specifications, which describe “the best way of doing something”, according to the knowledge and experience of experts in the subject considered [27]. This definition is proposed by the International Organization for Standardization (ISO), one of the most recognized entities for standardization. These frameworks can be defined by international organizations, such as the ISO [28]; but also by other entities, such as central governments [29].

While running audits or self-assessments allow organizations to understand the current status of their processes, keeping track of the processes changes and implement improvements along the time can be a challenge task to perform. To cope with this challenge, organizations can use maturity models to implement continuous improvement on target processes [30].

## 4.1. ISO/IEC 330xx

The ISO/IEC 330xx series of standards provides a structured approach for performing assessments, with the intent of guaranteeing that an assessment is objective, consistent, repeatable, and representative of the assessed processes [31].

One important concept in this series of standards is the Process Reference Model (PRM), a set of unifying processes that have each a description of its purpose and the associate outcomes [32]. Also, each process is described by its following attributes:

- **Process ID:** the identifier of the process
- **Name:** a short phrase that summarizes the scope of the process.
- **Context:** a brief overview of the context of process in the main subject.

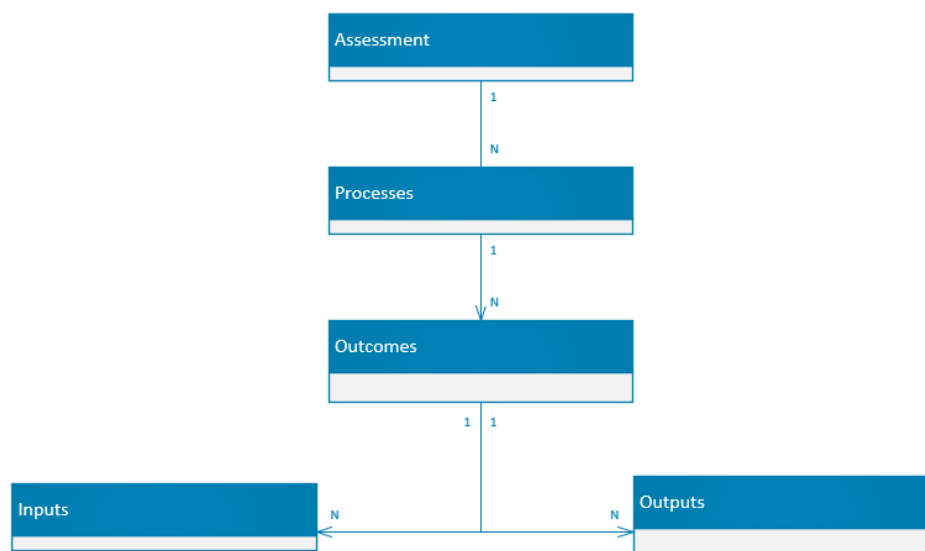
- **Purpose:** the high-level goal for the process.
- **Outcomes:** the observable results of a successful achievement related to the process.

Additionally, the capability of the processes described in a PRM is assessed by applying a Process Assessment Model (PAM), which describes the indicators needed to determine process capability and performance, such as generic practices; generic resources; and generic work products. These indicators are the basis for collecting evidence of the goals, which in turn allow the assessor to assign ratings and determine capability [33]. The capability dimensions included in PAMs are a six-point scale ranging from 0 to 5, where each level represents a specific process capability level:

- **Level 0:** Incomplete process
- **Level 1:** Performed process
- **Level 2:** Managed process
- **Level 3:** Established process
- **Level 4:** Predictable process
- **Level 5:** Innovating process

A PAM is directly related to one or more PRMs since it describes, for each process of a PRM, the fundamental indicators; base practices; and work products.

One of the best-known examples of the implementation of this standardization is the ISO/IEC 33052 (PRM) and the ISO/IEC TS 33072 (PAM) which provides a clear implementation for the ISO/IEC 27001, which provides requirements for information security management [34]–[36]. In Figure 4.1, we display the structure proposed by these two standards. For each assessment, the PRM established the processes and outcomes, while the PAM describes the inputs and outputs for each outcome.



**Figure 4.1.** Assessment structure proposed by the ISO/IEC 33052 and ISO/IEC TS 33072 standards

## 4.2. Commercial Tools

With the aim of better understanding which tools already exist in the market to support audit processes (which are often called compliance software), we investigated which commercial software tools are available and what are their associated functionalities.

To this end, we used Google search engine to search for the string “compliance software”. Considering that Google’s PageRank algorithm (for relevance ranking) shows the most relevant results in the first pages of the Google search, we considered the websites retrieved in the first page. We checked not only the tools’ webpages, but also webpages discussing the most relevant compliance management software tools.

After collecting the names of those tools, we checked their manufacturers’ website. We discarded tools that are specific to financial areas, such as SIPTA; since they are specialized in a specific segment of audits and cannot be generalized to other areas.

Then, we inspected the pages in the website where the tools’ functionalities were discussed. If available, we also studied their online demos to get a more in-depth insight on what these tools offered. For some tools, such as Compliance Management<sup>3</sup> e Teammate<sup>4</sup>, we could not find any information publicly available regarding their characteristics, and thus were not further considered in the analysis.

The software tools analysed are listed in Table 4.1, including their target users (organization employees or auditors); main functionalities; and main frameworks they target.

As we can see, even the information for the target users and the main frameworks is not always available. Nevertheless, we found that two tools were created for the organization, and one for the auditors. Regarding the frameworks, two tools provided support for multiple standards, while one is targeted for the ISO 9001 standard.

The most common functionality is the possibility to create reports (in four out of the six tools). In particular, BWISE allows to configure reports to display specific audit results. Three tools have functionalities to create workflows to automate processes.

Both BWISE and Quantivate allow to conduct risk assessments. Additionally, Standard Fusion also support overall risk management, and Microsoft Compliance Manager computes a risk-based compliance score based on the organization’s progress in completing improvement actions.

BWISE and ACL Galvanize Audit Management also offer means to create audit plans and to monitor their progress.

---

<sup>3</sup> **Compliance Management:** <https://www.wolterskluwer.com/en/solutions/enablon/compliance-management-software>

<sup>4</sup> **Teammate:** <https://www.wolterskluwer.com/en/solutions/teammate>

**Table 4.1.** Compliance Software Tools investigated

Name	Target	Main Functionalities	Main Framework
Microsoft Compliance Manager <sup>5</sup>	Organization	<ul style="list-style-type: none"> <li>• Workflow capabilities</li> <li>• Pre-built assessments</li> <li>• Step-by-step guidance on suggested improvement actions</li> <li>• Risk-based compliance score</li> </ul>	Generic standard approach (ISO 27001, NIST, GDPR)
Panotica Hydra 4.0 <sup>6</sup>		<ul style="list-style-type: none"> <li>• Reports</li> <li>• Audit manager</li> <li>• Document management</li> </ul>	ISO 9001
Standard Fusion <sup>7</sup>	Organization	<ul style="list-style-type: none"> <li>• Reports</li> <li>• Risk management</li> <li>• Audit manager</li> </ul>	Generic standard approach (ISO 27001, SOC2, NIST, HIPAA, GDPR, PCI-DSS, FedRAMP)
Quantivate <sup>8</sup>	Auditors	<ul style="list-style-type: none"> <li>• Reports</li> <li>• Workflow capabilities</li> <li>• Risk assessment</li> <li>• Map and apply regulatory requirements to other applicable artefacts (e.g. laws; processes; services)</li> <li>• Training and/or testing management</li> </ul>	
BWise <sup>9</sup>		<ul style="list-style-type: none"> <li>• Reports</li> <li>• Workflow capabilities</li> <li>• Risk assessment</li> <li>• Audit plans</li> <li>• Monitor progress</li> </ul>	
ACL Galvanize Audit Management <sup>10</sup>		<ul style="list-style-type: none"> <li>• Audit plans</li> <li>• Monitor progress</li> <li>• Data integration with other systems</li> </ul>	

<sup>5</sup> **Microsoft Compliance Manager:** <https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide> (Accessed 30/08/2021)

<sup>6</sup> **Panotica Hydra 4.0:** <https://www.hydra40.galactica.pl/en> (Accessed 20/09/2021)

<sup>7</sup> **Standard Fusion:** <https://go.standardfusion.com/compliance-software> (Accessed 20/09/2021)

<sup>8</sup> **Quantivate:** <https://quantivate.com/solutions/regulatory-compliance-management-software/> (Accessed 20/09/2021)

<sup>9</sup> **BWise:** <https://www.bwise.com/solutions/internal-audit/bwise-internal-audit> (Accessed 20/09/2021)

<sup>10</sup> **ACL Galvanize Audit Management:** <https://www.wegalvanize.com/> (Accessed 20/09/2021)



# 5. Literature Review

In this Chapter, we review some literature related to the research subject, namely regarding works investigating the use of software tools to support the audit processes. To achieve this goal, we conducted a SLR, as described in Section 5.1. First, we describe the planning phase of the SLR. Then, in Section 5.2 we present the results obtained by following the protocol. Finally, in Section 5.3 we answer the research questions that guide this review.

## 5.1. Planning

As described in Chapter 2, audit processes are very bureaucratic and based on manual procedures, often lacking objectivity and transparency. They are also subject to many biases. All this together represents major challenges for both assessors and organizations.

Therefore, with this SLR we aimed to understand the impact that the use of software tools can have on the assessors' work. Additionally, we also aimed to understand which tools (either software-based or not) were being used to support the audit processes, along with their characteristics.

### 5.1.1. Research Questions

Following the motivation and goals defined, this research work aims at answering the following research questions:

**RQ1.** Does the use of a software tool to support the audit processes can help assessors' organizing and optimizing their work?

- Which are the challenges being addressed?
- What are the evidences for the impact of software tools in audit processes?
- Which research methods are being used to evaluate the impact of software tools in audit processes?

**RQ2.** Which tools already exist to support audit processes?

- Which framework was addressed in this study?
- Which tool was used before introducing the proposed solution (if any)?
- Which base technology was used to develop the proposed solution?
- Which features were implemented in the proposed solution?
- Which stakeholders were considered for those tools?

### 5.1.2. Search Process

The search process started with the identification of the search string that should be used to capture all relevant papers. To assist on finding the search terms, the PICOC criteria [37] was defined for framing the literature as follows:

- **Population:** Assessor, Auditor

- **Intervention:** Assessment Management Tool, Software Assessment Tool, Assessment Process
- **Comparison:** does not apply
- **Outcome:** Efficiency, Productivity
- **Context:** Industry

Considering these terms, we selected the generic search string as follows: ("**Assessor**" OR "**Auditor**") AND ("**Assessment Management Tool**" OR "**Software Assessment Tool**") AND ("**Assessment Process**"). The terms included in the outcome and context were not included to avoid narrowing the research too much.

Then, the search string was applied to the title and abstract of the papers stored in the following digital libraries:

- **ACM Digital Library** (<http://portal.acm.org>)
- **AIS Electronic Library** (<https://aisel.aisnet.org/>)
- **EBSCO Host** (<http://eds.b.ebscohost.com/>)
- **IEEE Xplore** (<http://ieeexplore.ieee.org>)
- **ISI Web of Science** (<http://www.isiknowledge.com>)
- **Science@Direct** (<http://www.sciencedirect.com>)
- **Scopus** (<http://www.scopus.com>)

Additionally, all the primary papers selected from the digital libraries were analyzed using a snowballing strategy, as recommended by Webster and Watson [38] and based on Wohlin's guidelines [39]. We performed backward snowballing by analyzing the references of each primary paper, and forward snowballing by analyzing the citations to each primary paper, which were searched using Google Scholar.

The search was conducted on November 21st 2020 in the selected digital libraries, using the defined search string. Then, papers were screened based on the inclusion and exclusion criteria (which are presented in the next subsection). This screening activity started by discarding papers based on more practical issues. Then, the remaining papers were screened on the title and abstract. To finish, the remaining papers were screen based on its full text.

Next, the snowballing strategy was applied. Papers that have been previously examined and excluded in the process were discarded right away. Then, the inclusion and exclusion criteria were applied in three phases: first to the citation (including title, year, and venue), then to the paper's abstract, and finally to the full paper.

### 5.1.3. Inclusion and Exclusion Criteria

A set of inclusion and exclusion criteria was defined to filter the papers collected and identify the ones that were relevant for this work.

We developed the following inclusion criteria:

1. Clearly describes the impact of outcomes related to the use of technologies on the assessment management.
2. Clearly describes the problems that currently exists on the assessment management for all the stakeholders.
3. Empirical study included (qualitative or quantitative)
4. Focuses on assessment management using technological tools

Moreover, we excluded papers with the following features:

1. Duplicated document, including the same paper published in different databases and multiple publications refereeing to the same study and data.
2. Not written in English or Portuguese language.
3. Published before 2010. Considering the evolution of mobile technology, it makes sense to use these criteria in order to understand the impact of these platforms on the assessments.
4. Non-peer reviewed publication, except theses and dissertations.
5. Secondary and tertiary study.
6. Full-text not accessible.
7. Doesn't focuses on assessment management using technological tools.
8. Out of scope.

#### 5.1.4. Data Extraction and Synthesis

To answer the research questions, a data extraction form was designed and created on Parsifal, which was filled in for each of the papers selected. The data items and correspondent values that were extracted are the following:

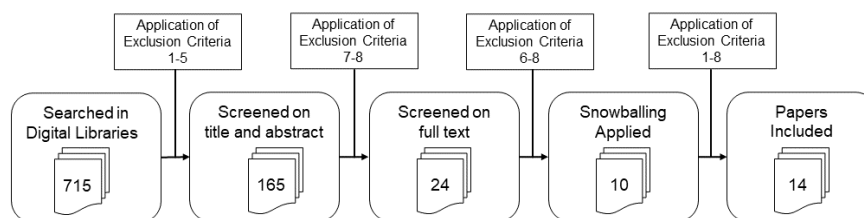
- **Challenges Addressed:** description of challenges addressed
- **Impact Observed:** description of impact observed
- **Research Type:** one of the following values, as proposed by Wieringa et al. [40]:
  - **Solution proposal:** a solution is proposed to a problem without providing a full validation.
  - **Evaluation:** the subject is investigated along with an empirical validation in practice (i.e. with real users in real settings).
  - **Validation:** the subject is investigated along with an empirical validation, but not in a practical setting.
- **Framework(s):** the frameworks that were addressed in this study.
- **Original Tool(s):** the tool that was used before introducing the proposed solution (if any)
- **Base Technology(ies) Used:** Technologies used to develop the proposed solution (if any)
- **Features:** Features that were implemented in the proposed solution.
- **Stakeholders:** The roles that were considered in the proposed solution.

The first three data items were allowed to answer RQ1, while the remaining were used to answer RQ2. Data extracted were tabulated and some graphics were created during the synthesis step, allowing to summarize relevant information, interpret results, and answer the research questions.

## 5.2. Conducting

This section describes the results obtained by conducting the SLR, using the protocol described in the previous section.

Initially, the search returned a total of 715 papers from the searches performed on seven digital libraries used for this SLR: ACM Digital Library (n=4); AIS Electronic Library (n=3); EBSCO Host (n=182); IEEE Digital Library (n=17); ISI Web of Science (n=113); Science@Direct (n=45); and Scopus (n=351). The iterative selection process described on the Figure 5.1 was implemented.



**Figure 5.1.** Paper selection process

As we can see, on the first step the exclusion criteria 1-5 were applied, which allowed to discard 550 papers. By analysing the title and abstract, on the second step was possible to exclude 141 papers, thus remaining 24 papers. Finally, the exclusions made on third step were based on the reading of the full papers, ending up with 10 valid papers.

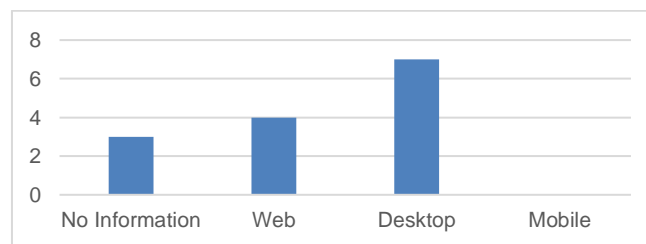
Considering that the number of valid papers were very low, it was imperative to understand if this number was a result of a lack of research in the area or if, on the other hand, it was due the search string was too generic to gather relevant papers for this study. To address this aspect, the snowballing strategy was performed to the 10 selected papers, and 22 additional papers were identified, which went through the selection process. In the end, 14 papers were included in this SLR, which are shown in Table 5.1.

As shown in Figure 5.2, the software tools described on the papers mainly focus on technologies target for the desktop operation systems (n=7). Also, a couple tools were made using web technologies (n=5) which allow the users to use them using a web browser. Finally, some of the papers doesn't include any reference of the technologies used (n=2) and also none of them were made using mobile technologies.

Another aspect was understanding which stakeholders were in focus on these studies. As shown on Table 5.2, we considered three categories: employees of the organization; assessors; and both. The results show that most studies focused only on the employees of the organization (n=6). Additionally, two studies focused on the assessors, and four focused on both the assessors and the employee of the organization.

**Table 5.1.** Studies included in the SLR

REF	Title	Author	Year
[1]	Assessing Software Processes over a New Generic Software Process Assessment Tool	Rasit Yurum, Ozan and Özcan-Top, Özden and Demirörs, Onur	2016
[33]	A three-dimensional innovation process capability assessment tool	Zhang, L. and Seidel, R. and Shahbazpour, M. and Haemmerle, E.	2013
[34]	Innovative decision support for IT service management	Shrestha, A. and Cater-Steel, A. and Toleman, M.	2016
[35]	CAT5: A Tool for Measuring the Maturity Level of Information Technology Governance Using COBIT 5 Framework	El Houssaini, Souhail El Ghazi and Youssef, Karim and Boutahar, Jaouad	2016
[36]	Software process capability self-assessment support system based on task and work product characteristics: A case study of ISO/IEC 29110 standard	Methawachananont, A. and Buranarach, M. and Amsuriya, P. and Chaimongkhon, S. and Krairaksa, K. and Supnithi, T.	2020
[37]	Building a software tool for transparent and efficient process assessments in IT Service Management	Shrestha, A. and Cater-Steel, A. and Toleman, M. and Tan, W.-G.	2014
[38]	SPIALS: A light-weight software process improvement self-assessment tool	Homchuenchom, D. and Piyabunditkul, C. and Lichter, H. and Anwar, T.	2011
[39]	An application tool to support the implementation of integrated software process improvement for Malaysia's SME	Ali, R.Z.R.M. and Ibrahim, S.	2011
[40]	TMM Appraisal Assistant Tool	Tayamanon, T. and Suwannasart, T. and Wongchingchai, N. and Methawachananont, A.	2011
[41]	An Ontology Based Infrastructure To Support CMMI-Based Software Process Assessment	Gazel, Sema and Sezer, Ebru Akçapinar and Tarhan, Ayca	2012
[42]	Mapping Process Capability Models to Support Integrated Software Process Assessments	Marcello, Thiry and Alessandra, Zoucas and Leonardo, Tristão	2018
[43]	Avalia-MMPE: uma ferramenta para suporte a avaliações no MMPE-SI/TI (Gov) com foco no usuário	Araújo, Leonardo Cordeiro de	2013
[44]	Assess Agility: An Agility Assessment Approach Supported With An Automated Web Based Agility Assessment Tool	Adali, onat ege	2017
[45]	GSPA: a generic software process assessment tool	Yürüm, Ozan Raşit	2014



**Figure 5.2.** Technologies used in the selected papers

**Table 5.2.** Stakeholders in focus in selected papers

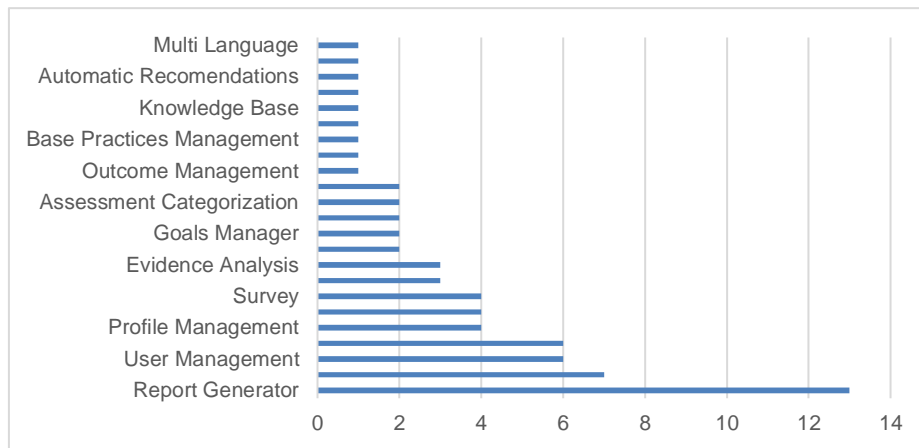
Stakeholders	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14
Employees of organization		X		X	X	X	X	X		X		X	X	X
Assessors			X					X	X	X	X	X	X	
No Information	X													

Table 5.3 lists the frameworks and maturity models that these tools were based on. The results are quite sparse, which clearly indicates that there is one framework nor maturity model that is being considered when developing these tools. Still, the ISO/IEC 15504 standard (N=4) and the CMMI maturity model (considering all views or specifically the Development view) (N=4) were the most referred.

**Table 5.3.** Frameworks and maturity models supported by the tools studied in selected papers.

Framework/Model	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14
COBIT 5			X											
ISO/IEC 29110				X										
ISO/IEC 15504					X		X			X				X
MPS.BR										X				
ISO/IEC 2500												X		
ISO/IEC 155042		X									X			
ITIL		X												
ISO/IEC 20000		X												
Testing Maturity Model								X						
CMMI Development										X	X			
CMMI						X							X	
MMPE-SI/T												X		
AgilityMod													X	
CMM	X													
Other									X					

The most common functionalities of the proposed software tools identified are listed in Figure 5.3 and Table 5.4. The results show that the reporting generator (N=13), rating system (N=7), user management (N=6) and possibility to upload evidences (N=6) were the most common functionalities available in these software tools.



**Figure 5.3.** Most common functionalities

**Table 5.4.** Functionalities

Functionalities	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14
Report Generator		X	X	X	X	X	X	X	X	X	X	X	X	X
Rating System				X	X		X	X	X	X	X			
User Management		X				X	X			X		X	X	
Upload Evidence				X				X		X	X	X		X
Profile Management						X	X					X	X	
Processes management		X			X		X		X					
Survey		X	X		X	X								
Rate Process		X				X						X		
Evidence analysis			X		X			X						
Organization Management									X			X		
Goals Manager									X			X		
Process Categorization					X				X					
Assessment Categorization					X						X			
Multi Assessments							X				X			
Outcome management		X												
Report and Analysis Management			X											
Base Practice Manager									X					
Frameworks Management											X			
Knowledge base		X												
Gap Analysis							X							
Automatic Recommendations					X									
Multi framework											X			
Multi Language												X		

In Table 5.5, the challenges that the selected studied tried to address using the proposed solutions are listed. The challenge most commonly reported is the lack of transparency and efficacy of the assessments (N=3), followed by the high costs of the assessments (N=2) and the difficulty on maintain a software targeted for the process assessments (N=2).

**Table 5.5.** Target challenges considered in the selected studies

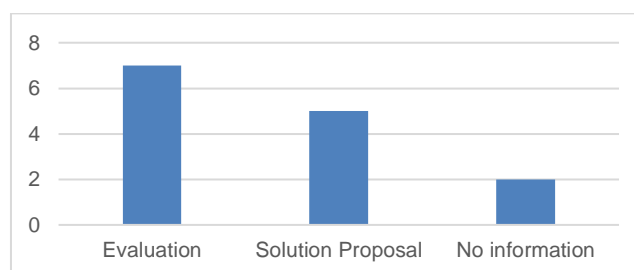
Challenges	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14
Lack of transparent and efficient process assessment methods	X	X			X									
High costs in assessments for small and very small companies						X	X							
Difficulty on maintaining software process assessments										X	X			
Complex assessments								X						
Lack of focus on usability									X					
Lack of tools that multiple audits to be done in several framework												X		
Lack of self-awareness													X	

The results obtained in these studies were diverse, since the solutions proposals also differ concerning the scope and goals. The results can be divided in two types: those who had either positive impact (n=5) or negative impact (n=6). Some outputs were similar between studies, such as the lack of functionalities available (N=3) and the increase in the capability of the auditor (N=3), as shown in Table 5.6.

**Table 5.6.** Results observed in the selected studies. Greyed rows correspond to positive results.

Results observed	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14
Report useful		X			X									X
Better decision making		X												X
Gather information more easily					X								X	
Cheaper Audits					X									
Auditor performance increased											X		X	X
Information missing											X	X		X
Functionalities missing												X	X	X
Parallel assessment not possible											X			
UI/UX problems												X		
Insufficient Response Time												X		
Time consuming report		X												

As we can see in Figure 5.4, most of the papers in study used the research evaluation method (N=7) the rest of the papers used Solution proposal (n=5).



**Figure 5.4.** Research methods applied in the selected papers



### 5.3. Reporting

In this Section, we discuss the answers to the two defined research questions.

#### 5.3.1. Does the use of a software tool to support the audit processes can help assessors’ organizing and optimizing their work?

Based on the evidence gathered with this SLR, software tools seem to be useful to assist in many aspects of the auditing process. For example, having reporting functionalities seems to allow stakeholders to enhance the decision-making process.

Another important topic was the noticeable increase of performance in the assessors’ work, which was reported in several papers. This happens mainly because the software tools allowed the assessors to gather the evidence (and thus, the information) needed to conduct the audits in an easier way, when compared to a scenario where no software tool was used. Also, having tools to manage the agenda of the audit processes contributed to the improvement of audits’ performance since it allowed to create appointments more easily with the stakeholders relevant to the topic(s) being analyzed.

#### 5.3.2. Which tools already exist to support audit processes?

The main characteristics of the tools identified in the SLR are summarized in Table 5.7. Hence, we will be referring to software tools, since no analogic tool was discussed to in the selected papers.

The software tools found during the SLR can be divided in two categories, according to the target users: the ones intended to be used only by the assessors, and the other ones intended to be used by both the assessors and the organization that is being audited.

Because these tools have different target users, their goals and structure are different. While the first try only to organize the auditor work, maintaining the traditional process to run audits, the other tries to transform the auditing processes using technology.

**Table 5.7.** Summary of the identified tools’ characteristics.

	Target Users	
	Assessors	Assessors and Organization Audited
<b>Main Goal</b>	Organize the auditors’ work in the traditional auditing process	Digitalize the auditing process
<b>Main Functionalities</b>	<ul style="list-style-type: none"> <li>• Meeting Schedule</li> <li>• Evidence Upload</li> <li>• Assessments’ Rating</li> </ul>	<ul style="list-style-type: none"> <li>• Form fulfilment</li> </ul>
<b>Technology(ies) used</b>	<ul style="list-style-type: none"> <li>• Desktop applications</li> <li>• Web applications</li> </ul>	
<b>Frameworks considered</b>	Generic frameworks that apply to different standards	

For the first type of software tools, the main functionalities were: the meeting scheduling; upload of evidences; and a rating system for the assessments. The second type of tools were more focused on the tasks that the organizations' stakeholders can do to help and facilitate the assessor work. In that sense, functionalities like form fulfilment (for gathering information without the need to run meetings) can improve the efficiency of the assessments.

As for the technologies used, most software tools were developed directly for desktop environments, which lacks some versatility, since the auditor always need access to a computer to use them. The second most common type of applications were the ones made using web technologies, which is more flexible, since assessors can use them in any device with a browser.

Regarding the frameworks that these tools support, a significant part of these software tools are based on a proposed generic framework, based on the ISO/IEC 15504 and/or the CMMI maturity model. This enables the auditor to keep record of multiple assessments for various already existent frameworks. However, creating a tool that is generic enough to support all these frameworks is a task complex and hard to perform. Thereby, most of the identified tools focus in specific frameworks

# 6. Proposal

In this chapter, we describe the specific objectives and the proposal that was developed to address the research problem.

## 6.1. Objectives

The main goals of this research proposal are the following:

- Provide more support for auditors to conduct audits and perform their work;
- Improve the audit processes using software tools.

## 6.2. Description

To achieve the defined objectives and address the underlying research problem, we proposed the development of two artefacts: a model and its instantiation. More specifically, these artefacts consist of a **software tool that will help an assessor to determine the capability of a process in a concise and efficient way**. The model is described during the remainder of this Chapter, while its instantiation will be detailed in Chapter 7.

This software tool centralizes all the main tasks that an assessor does, such as collecting evidence; rating processes' capabilities based on that evidence; and schedule meetings with employees in the organization. Furthermore, this tool was intended to improve the audit processes in the following ways:

- Organizing and optimizing the assessors' work;
- Improving the efficiency and effectiveness of those processes;
- Reducing the associated costs.

The model was created through different phases. The first step was to establish the requirements for the tool, based on the work performed so far (and already described in previous Chapters of this document). To start with, the research team discussed some ideas for the tool based on the insights collected with experienced auditors (as described in Section 2.1); the specification of the ISO/IEC 33052 and ISO/IEC 33072 standards [41], [42].; the commercial tools analysed; and the related works discussed in this document. A summary of the tasks/functionalities proposed is displayed in Table 6.1.

The initial goal was to create a model that was simple to implement, so that we could validate it as soon as possible. First, we needed to create the base structure to support the audit process, based on Figure 4.1. Then, we further decided to implement the support to schedule meetings, and the assessments' rating system.

The other functionalities were not considered in a first stage, because while widely mentioned (such as the reports), since they were more advanced, and we wanted to validate the base structure first.

As a result, the following set of relevant and important functionalities were selected for the tool:

**Table 6.1.** Tasks performed by the auditors and functionalities proposed for a software tool, mentioned in each research method

	Interviews with Experts	SLR	Commercial Tools
Reports	X	X	X
Create audit plans	X		X
Forms to gather information	X	X	
Evidences management	X	X	
Meeting Schedule	X	X	
Define stakeholders for each process being audited	X		
Continuous Improvement	X		
Set responsible by process	X		
Assessments Rating		X	
Workflows			X
Risk assessment			X
Monitor audit progress			X

1. Create organization and associate employees;
2. Meeting scheduling associated with employees;
3. Creation of a new assessment;
4. Add evidence to an outcome;
5. Evaluate processes based on the rate of outcomes;
6. Evaluate outcomes based on the evidence;
7. Insert frameworks individually
8. Insert frameworks bulk (back-office functionality)

The functionalities 1-3 and 7-8 correspond to the preparation of the audit, while functionalities 4-6 correspond to its execution. Functionalities related to inserting and visualizing base practices were left out of this proposal, since they are less relevant to the auditor when compared to the ones listed.

The final requirements of the tool are presented on Table 6.2, grouped into categories, according to the entity related to audits that they are focused on creating and managing: *Organization*; *Framework*; *Assessment* and *Meeting Schedule*. The requirements in category *Users* are related to the users' management in the application.

Afterwards, the UML class diagram was created, which is shown in Figure 6.1. This model was created based on the ISO/IEC 33XXX family of standards, so that the application data could be handled [41]. This model also shapes the database structure of the model.

With the tool structure defined, and considering the feedback provided by the auditors interviewed in Chapter 2, we created an activity diagram representing the flow of each of the selected functionalities. To simplify the first version of the tool, we decided not to include support for adding the inputs and outputs, although they are included in the UML diagram (for latter implementation).

**Table 6.2.** Tool requirements.

Category	Title	Requirement
Organization	Create organization	The system should allow the users to create new organizations in the system.
	Create employees	The system should allow the users to create new employees and associate them with an organization.
	Edit organization	The system should allow the users to edit an organization already created.
	Delete organization	The system should allow the users to delete an organization already created.
	Search organization	The system should allow the users to search by an organization
Framework	Create a framework	The system should allow the users to create a new framework
	Edit a framework	The system should allow the users to edit all the components of a selected framework (framework information, processes, outcomes, inputs, and outputs)
	Delete a framework	The system should allow the users to delete a framework already inserted.
	Search frameworks	The system should allow the users to search by frameworks.
Assessment	Create new assessment	The system should allow the users to create a new assessment
	Rate processes	The system should allow the users to rate processes of an assessment
	Rate outcomes	The system should allow the users to rate an outcome
	Upload evidence	The system should allow the users to upload evidence to a specific outcome
Meeting Schedule	Create a new meeting	The system should allow the users to schedule a new meeting.
	Associate users to a meeting	The system should allow the users to associate employees of an organization to a specific meeting already created
	Edit meeting	The system should allow the users to edit a meeting already created
	Delete meeting	The system should allow the users to delete a meeting already created.
Users	Create users	The system should allow the administrators to create new users
	Edit users	The system should allow the administrators to edit a user's information
	Delete users	The system should allow the administrators to delete a user

For the first functionality, creation of an organization, the activity diagram presented in Figure 6.2 was created. This simple functionality allows the auditor to create a new organization in the application. For that, the auditor needs to input the basic information of the organization and then create new employees.

The meeting scheduling functionality allows the auditor to create new appointments with other people associated with a specific organization and assessment, as shown in Figure 6.3. The assessor must fill in the basic information of the meeting, such as the start and end date of the event and the subjects that will be discussed. Then, (s)he must associate employees to that meeting, which will allow the application to send emails for each one of them informing them of the new appointment.

The activity diagram in Figure 6.4 describes the steps linked with functionality 3: creating an assessment. For that, the assessor must first select the organization (s)he is going to audit, and the framework considered.

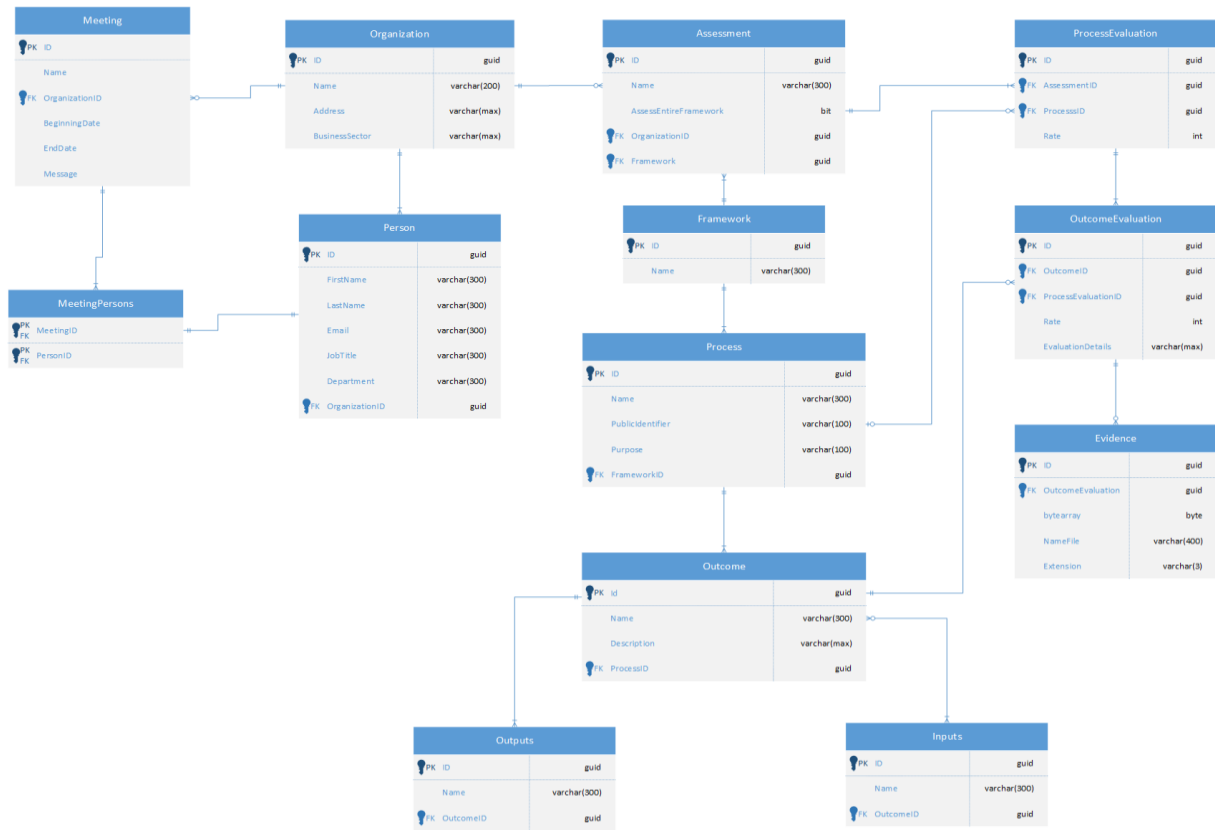


Figure 6.1. UML diagram of the software tool

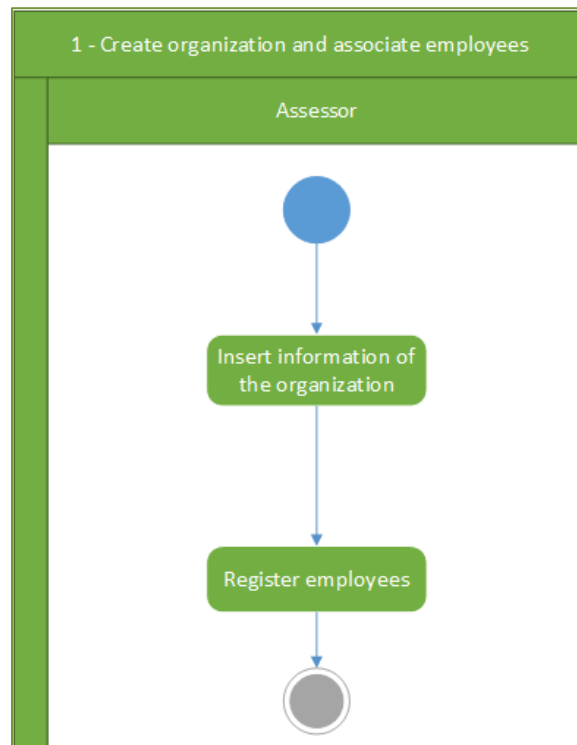
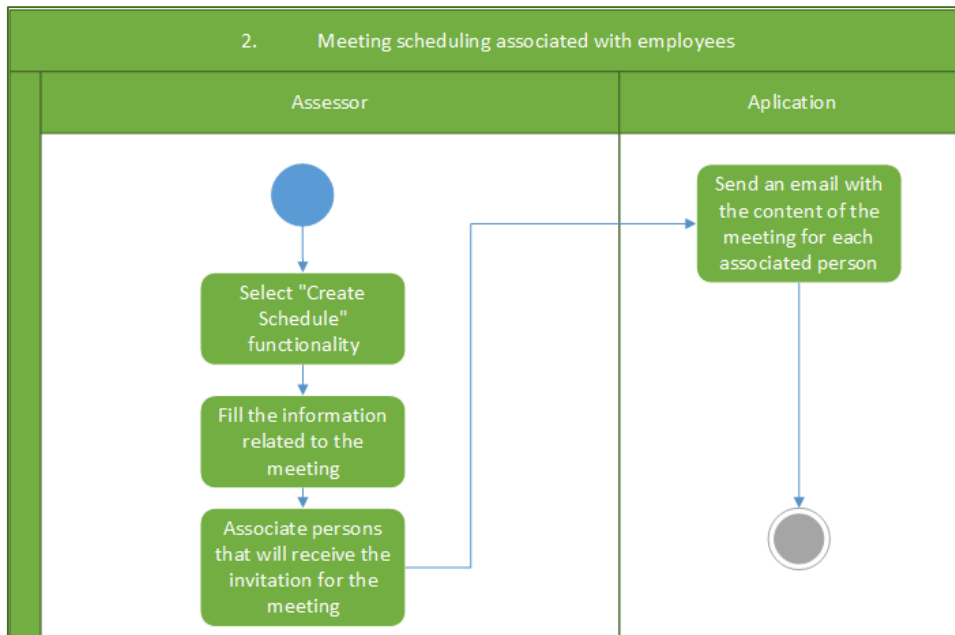
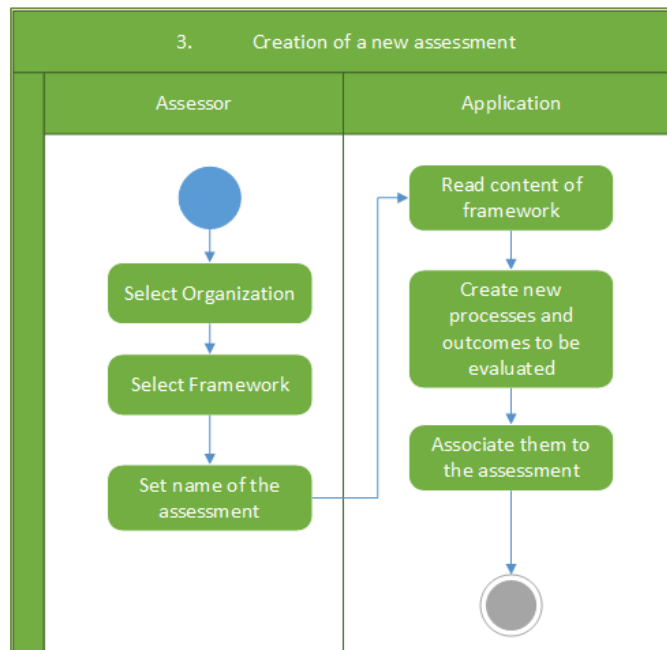


Figure 6.2. Create Organization – Functionality Activity Diagram

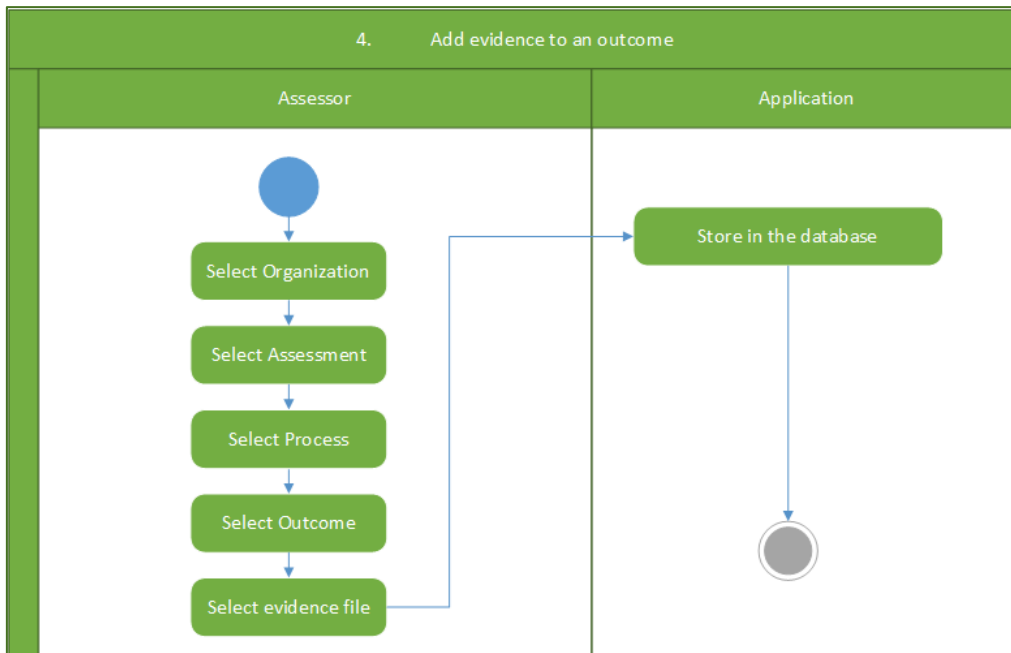


**Figure 6.3.** Meeting scheduling – Functionality Activity Diagram

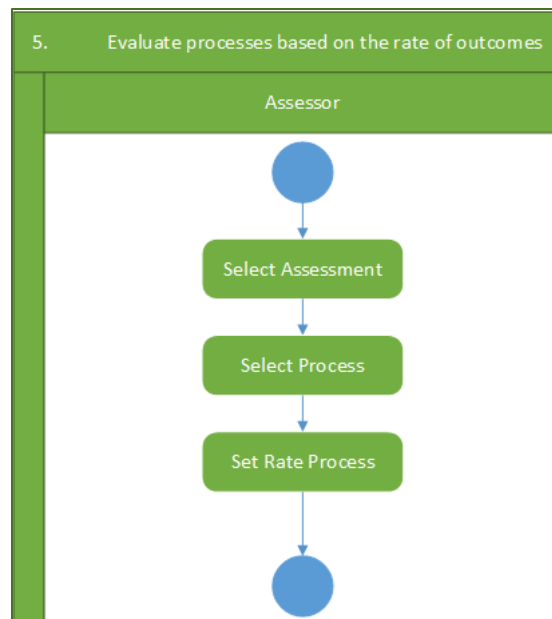


**Figure 6.4.** Create new assessment – Functionality Activity Diagram

To add evidence to an outcome (functionality 4), the assessor needs to first select the assessment; the process; and an outcome to upload the evidence, as shown in Figure 6.5. Then, to evaluate a process (functionality 5), the assessor needs to choose the assessment; and the process that (s)he wants to rate - as shown in Figure 6.6.



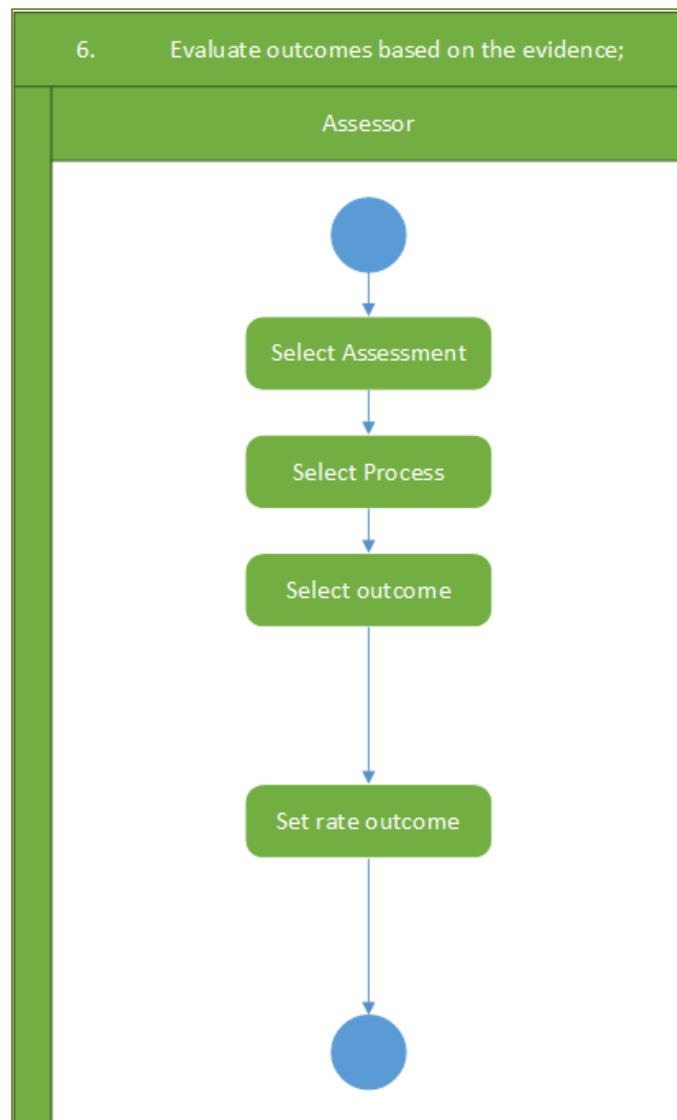
**Figure 6.5.** Add evidence to an outcome – Functionality Activity Diagram



**Figure 6.6.** Evaluate process based on evidence – Functionality Activity Diagram

For a process to be evaluated correctly, the outcomes associated to that process must be evaluated properly, which corresponds to functionality 6 of the proposed model, whose activity diagram is shown on Figure 6.7. To achieve that, the assessor must access the assessment, then select the process and the outcome that will be evaluated.



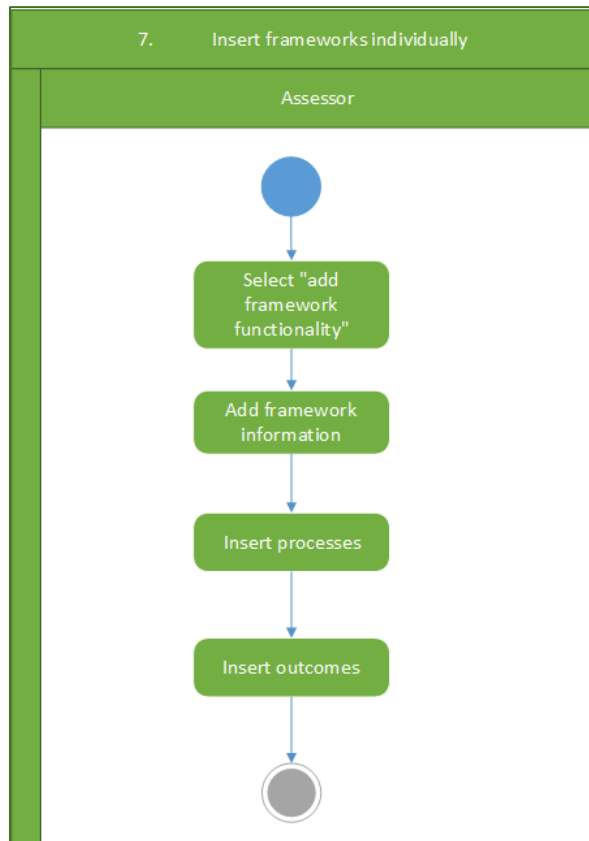


**Figure 6.7.** Evaluate outcomes based on evidence – Functionality Activity Diagram

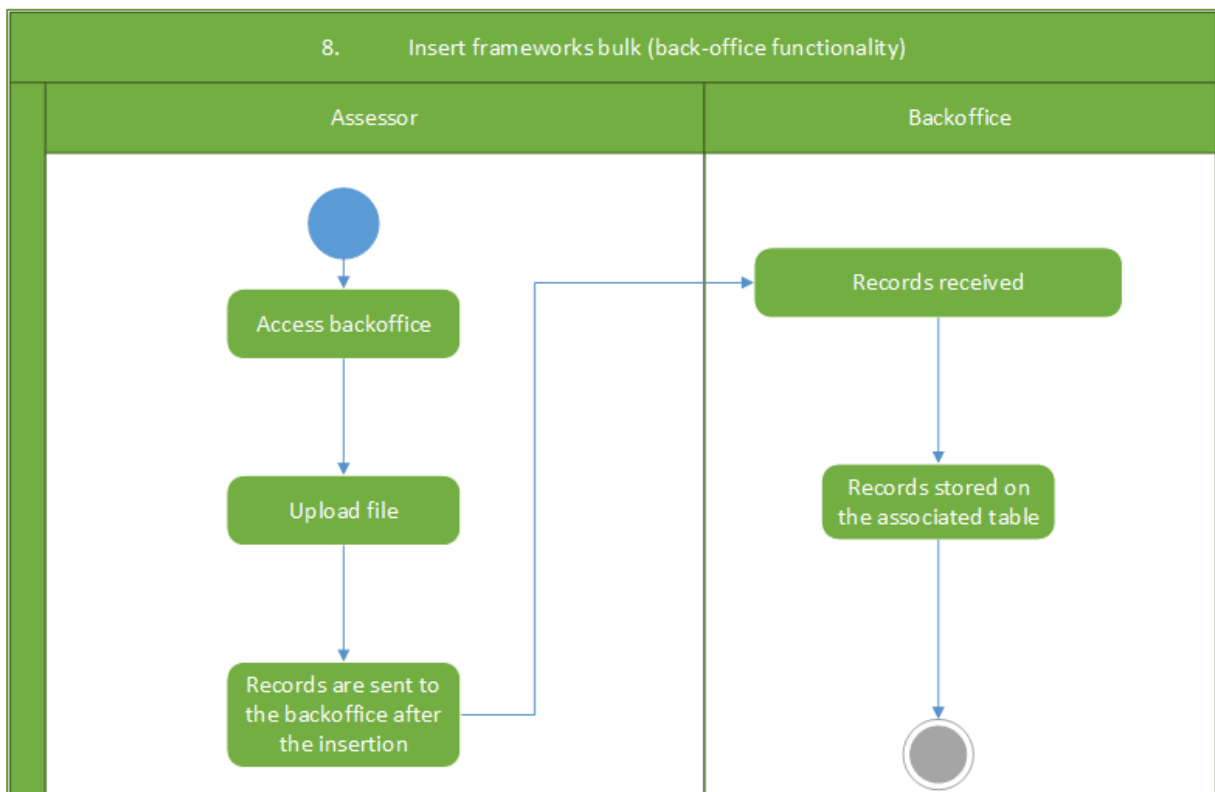
The insertion of frameworks on the application can be done in two different ways: either using the front end or the back-office. To insert a framework using the front end, the user must fill the basic information of the framework within the application, as shown in Figure 6.8. Then, for each process of the framework, the user inserts the process, and then creates the outcomes associated with that process.

The back-office functionality must allow the insertion of standards in bulk and should only be accessible by the admins. More specifically, the admin must be able to upload a file containing all the information for one or more frameworks (following the structure of the ISO/IEC 33052 and ISO/IEC 33072 standards), which in turn should populate the database. This process is displayed in Figure 6.9.

In the next Chapter, we will describe how this model was instantiated into a functional prototype.



**Figure 6.8.** Insert frameworks individually, using the front end – Functionality Activity Diagram



**Figure 6.9.** Insert frameworks in bulk, using the backoffice – Functionality Activity Diagram

# 7. Demonstration

In this section, which corresponds to the demonstration step of the DSR approach, we show how the proposed solution can be used to address the identified research problem.

The model artefact was instantiated as a prototype, which was loaded with two frameworks. Based on the feedback received during the evaluation of the first version of the tool (as described in the following Chapter), the tool was refined into an improved version. These activities are described in the following Sections.

## 7.1. Tool Prototype

The proposed model (described in Chapter 6) was instantiated into a prototype using Microsoft Power Apps technologies<sup>11</sup>. More specifically, a web application was developed, since the versatility allowed by such tools could ease the auditors' work, who could use it on desktop computer and/or on a mobile platform.

The first step consisted on creating a new Microsoft PowerApps subscription to host the application. Then, the Microsoft Data verse database was customized to support the requirements of the application. Custom entities were created to handle the data needed to support the planned functionalities, as illustrated on the class diagram presented in Figure 6.1. After the database was fully customized, the functionalities' web pages were created, according to the model defined and as described below.

When creating an application using PowerApps, the login page is created automatically, as shown in Figure 7.1. The auditor can log into the portal using one of multi-methods of authentication available in PowerApps. First, the user can use the internal credentials system by providing a username and a password to authenticate. In alternative, if the user has a Microsoft account, these credentials could be used. This is possible because the tool was also integrated with Microsoft accounts, taking advantage of the support of the open id connect protocol.

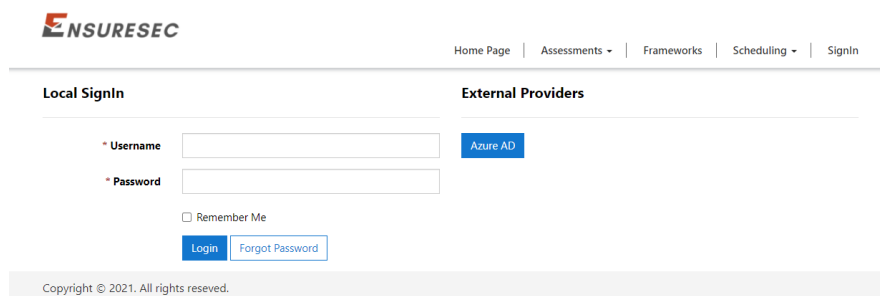
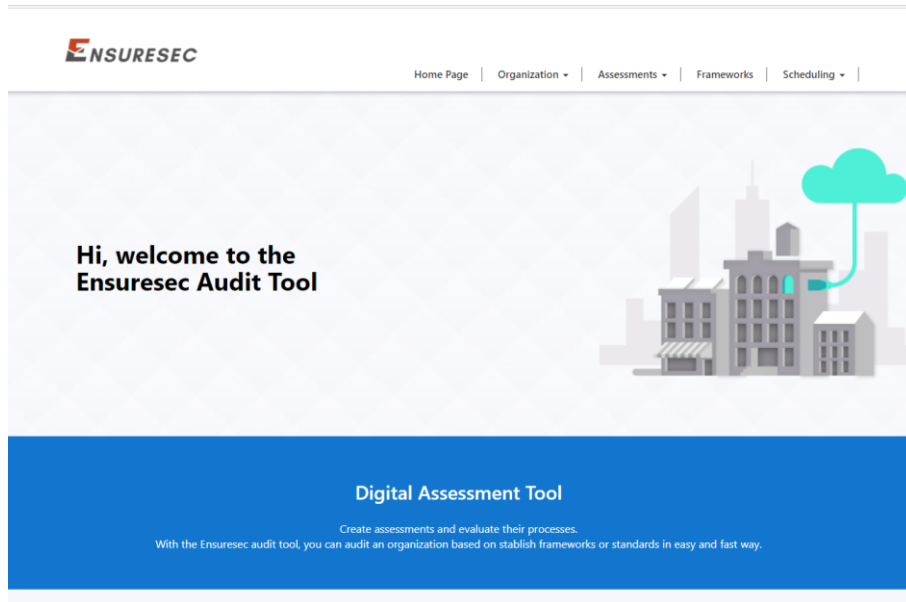


Figure 7.1. Login page of the application

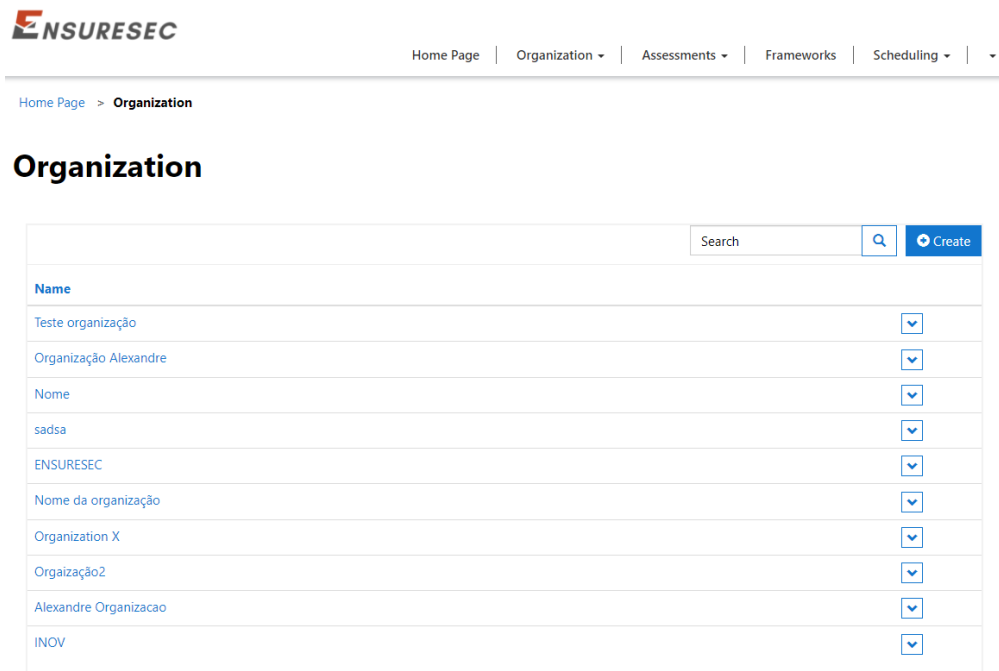
<sup>11</sup> Microsoft Power Apps: <https://powerapps.microsoft.com/pt-pt/> (Accessed on 17/01/2021)

After being authenticated on the portal, the tool redirects to the homepage (shown in Figure 7.2), containing generic information about the tool and details on how it can be used.



**Figure 7.2.** Homepage of the application

One of the areas available in the tool is the one related to the organization information. Figure 7.3 shows the list of all organizations that were inserted by an user. From here, a new organization can be created (by clicking on the “Create” button on the top right of the list) or an already existent one can be edited, by clicking on its name.



**Figure 7.3.** List of organizations

The page for creating an organization is shown in Figure 7.4, which allows to insert both general information and to associate employees.

**Figure 7.4.** Page for creating an organization

The application also has a schedule manager, where an auditor can see a list of all the meetings that have already been created, as shown in Figure 7.5.

Name	Organization	Beginning Date	End Date
TEste		3/20/2021 2:22 PM	3/25/2021 2:22 PM
TEste 2		3/1/2021 2:59 PM	3/11/2021 2:59 PM
Reunião 22		3/25/2021 6:46 PM	3/19/2021 6:46 PM
TEste		4/15/2021 8:43 PM	4/14/2021 8:43 PM
titulo		4/28/2021 5:46 PM	4/28/2021 5:46 PM
sadsa		5/4/2021 11:25 PM	5/15/2021 11:25 PM
123		5/4/2021 2:24 PM	5/6/2021 2:24 PM
Discussao Prcesso A		5/13/2021 3:18 PM	5/13/2021 3:18 PM
TEste		5/19/2021 5:15 PM	5/13/2021 5:15 PM
sadsa		5/3/2021 5:16 PM	5/12/2021 5:16 PM

**Figure 7.5.** List of meetings scheduled

By clicking on the “Create” button on the top right of that list, the user is redirected to a page (shown in Figure 7.6) where he can add the general details of a meeting and associated employees.

## Create Schedule

Schedule Information
Associate Persons

**Title \***

**Beginning Date \***

**End Date \***

**Organization**

**Message**

Submit

**Figure 7.6.** Create a schedule for a meeting.

All assessments created are listed on the page shown in Figure 7.7. Assessments can be filtered by either organization or framework, and new assessments can be created by clicking on the “Create” button on the top right of the list.

## Assessments

**Organization**

▼

**Framework**

▼

🔍

Create

Name	Framework	Organization	Created on ↓	▼
Auditoria 27001 27/08	ISO/IEC TS 27001	Organizaçao Alexandre	8/27/2021 6:09 PM	▼
Auditoria ISO 27001 23/08	ISO/IEC TS 27001	Alexandre Organizacao	8/23/2021 6:34 PM	▼
Iso 27001 19/08	ISO/IEC TS 27001	ENSURESEC	8/19/2021 10:05 AM	▼
Auditoria 27001 - 13/08	ISO/IEC TS 27001	Nome da organizaçao	8/13/2021 5:46 PM	▼
Auditoria 27001 30/07	ISO/IEC TS 27001	INOV	7/30/2021 6:48 PM	▼
Assessment	DT Framework	Organization X	7/6/2021 4:18 AM	▼
Iso 27001 -02/07	ISO/IEC TS 27001	INOV	7/2/2021 3:17 PM	▼
ENSURESEC	Process Assessment Model for Business Continuity Management	ENSURESEC	6/30/2021 3:27 PM	▼
Ensuresec	Process Assessment Model for Business Continuity Management	ENSURESEC	6/30/2021 3:05 PM	▼

Apply

**Figure 7.7.** List of assessments

By clicking on the name of an assessment, the user is redirected to the page shown in Figure 7.8, where the information for a specific assessment can be edited. Additionally to some generic information (such

as the framework and organization it corresponds to), the list of processes associated with the assessment is shown, which can be filtered to only display either open or closed processes.

## Edit Assessment

[Assessments](#) > [Edit Assessment](#)

**Assessment \***  
Auditoria 27001 27/08

**Framework**  
ISO/IEC TS 27001

**Organization**  
Organização Alexandre

**Assess full framework? \***  
 No  Yes

**ProcessEvaluation**  
[Open Processes ▾](#)

Process ↑	Created on	
Asset management	8/27/2021 6:09 PM	▾
Capacity management	8/27/2021 6:09 PM	▾

**Figure 7.8.** Edit assessment page

When selecting a specific process, the tool redirects to the page displayed in Figure 7.9, where a process can be rated; a list of the process' outcomes that are open or close can be seen; and a new outcome can be added. When rating the process (functionality 5), one of the following levels (listed in Section 4.1) can be selected: incomplete (0); performed (1); managed (2); established (3); predictable (4); innovating (5).

When a specific outcome is accessed (by clicking on its name), the tool is redirected to the page shown in Figure 7.10, where the user can provide details about the evaluation being conducted; rate the outcome; and upload evidence to support that rate. When rating the outcome (functionality 6), one of the following options can be selected:

- Not achieved (0-15%)
- Partially achieved (>15-50%)
- Largely achieved (>50-85%)
- Achieved (>50-85%)
- Fully achieved (>85-100%)

## Edit Process of Assessment

Assessments > Edit Process of Assessment

**Process \***  
Asset management

**Rate**

**OutcomeEvaluation**  
[Open Outcomes ▾](#)

Number ↑	Name	Rate
	Items requiring asset management are identified	<input type="text"/>
	Asset items are classified	<input type="text"/>
	[The status of assets is identified.]	<input type="text"/>
	Assets are inventoried	<input type="text"/>
	Changes to assets under management are controlled.	<input type="text"/>

[Submit](#)

Figure 7.9. Edit a process associated to an assessment

## Edit Outcome of Process

Assessments > Edit Outcome of Process

**Outcome \***  
Items requiring asset management are identified

**Rate**

**Evaluation Details**

**Edit Evidences**  
[+ Create](#)

Name ↑	Created on
There are no records to display.	

Figure 7.10. Edit the outcome of a process that is associated to an assessment



## 7.1.1. Framework Loading

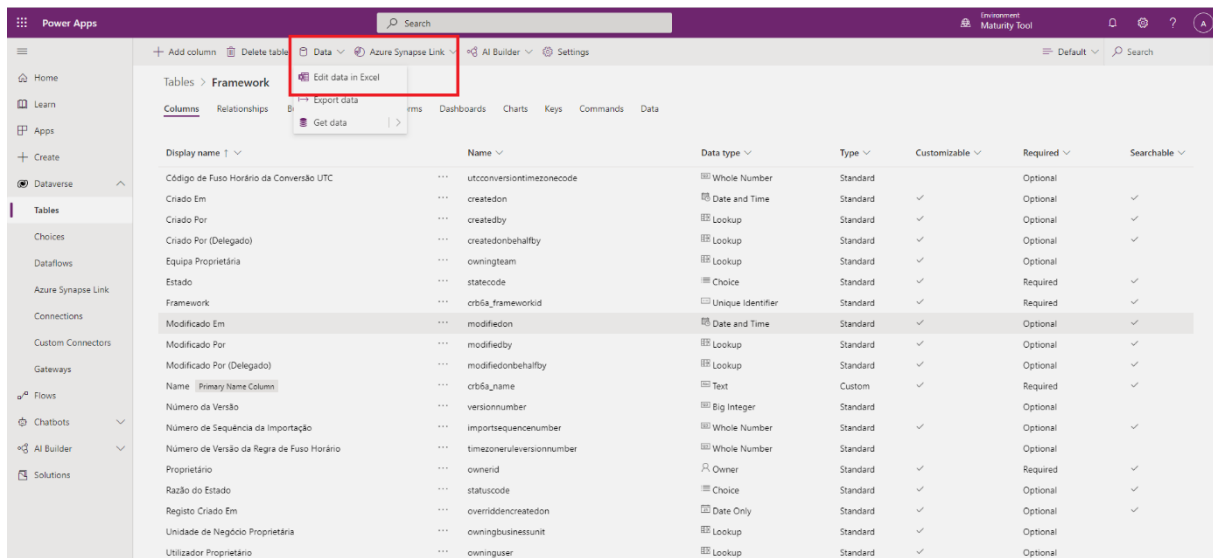
One of the functionalities of this tool is the ability to import any framework that follows the same structure of the ISO/IEC 330xx series of standards to the application. In this way, we can guarantee the flexibility of the tool itself, making it able to be used on multiple use cases.

As previously explained in Chapter 6, the application has two methods for loading frameworks: insert an individual framework using the front end; and insert frameworks in bulk using the back-office functionality.

For the back-office functionality, we took advantage of the mechanisms available in the PowerApps technology, which allows to insert data on the application tables using one of two sources: an Excel file or external databases. In both cases, it is necessary to map the fields of the application tables to those of the Excel columns/external database tables. When that connection is established, the user can insert information of multiple frameworks at once.

We demonstrated this functionality by uploading two different frameworks: the PRM and PAM of the ISO/IEC 27001 (ISO/IEC 3305 and ISO/IEC 33072, respectively), and a digital transformation maturity model. This digital transformation maturity model aims to guide organizations through their digital transformation initiatives, and was developed according to the ISO/IEC 330xx family of standards. As in the PRM and PAM of ISO/IEC 27001, the ISO/IEC 3305 and ISO/IEC 33072 standards were followed.

In both cases, we started by inserting the name of the framework on the back-office. Then, we selected the table where the data was to be inserted in the back office, and selected the option “Edit data in Excel” (as shown in Figure 7.11 for the *Process* table).



**Figure 7.11.** PowerApps backoffice where the table *Process* is accessed, with the “Edit data in Excel” option highlighted with a red rectangle.

The records corresponding to that table are then inserted into the Excel file (as shown in Figure 7.12 for the *Process* table), and in the end recorded in the application's database, thus becoming available for the auditor to use. This process is repeated for the tables *Framework*, *Process* and *Outcome*.

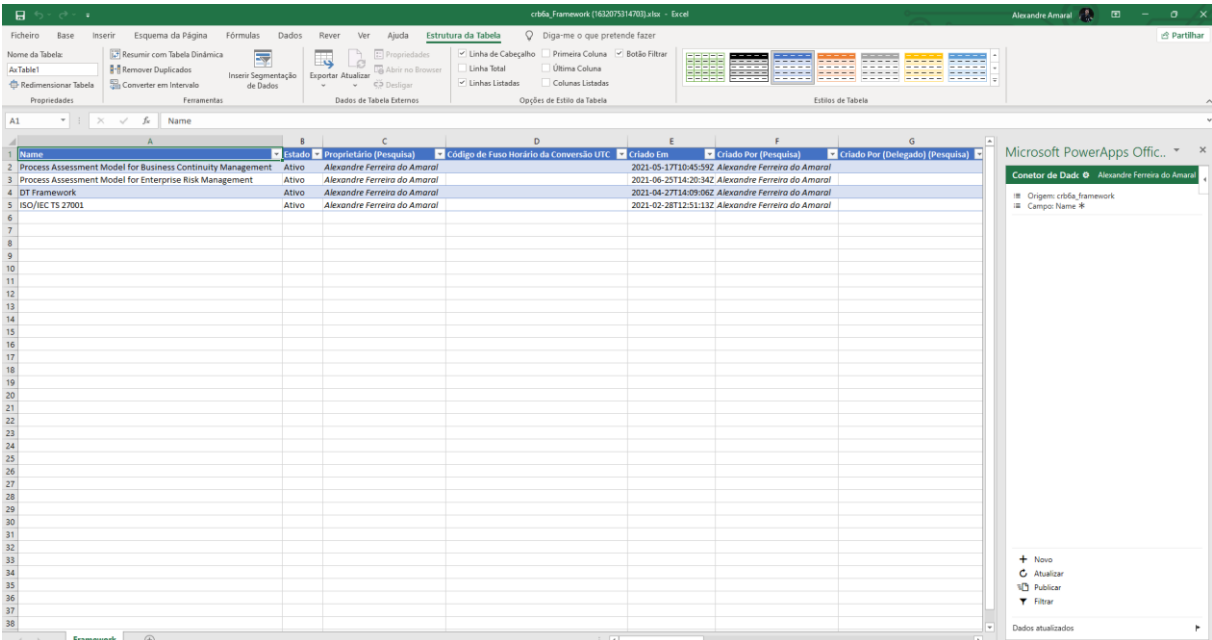


Figure 7.12. Excel file containing the information for the *Process* table of the application database

Afterwards, both frameworks were listed in the application, as shown in Figure 7.13. In both cases, the process underwent with no issues, thus demonstrating that two frameworks with distinct purposes (but a common underlying structure) can be uploaded to this same, generic tool.

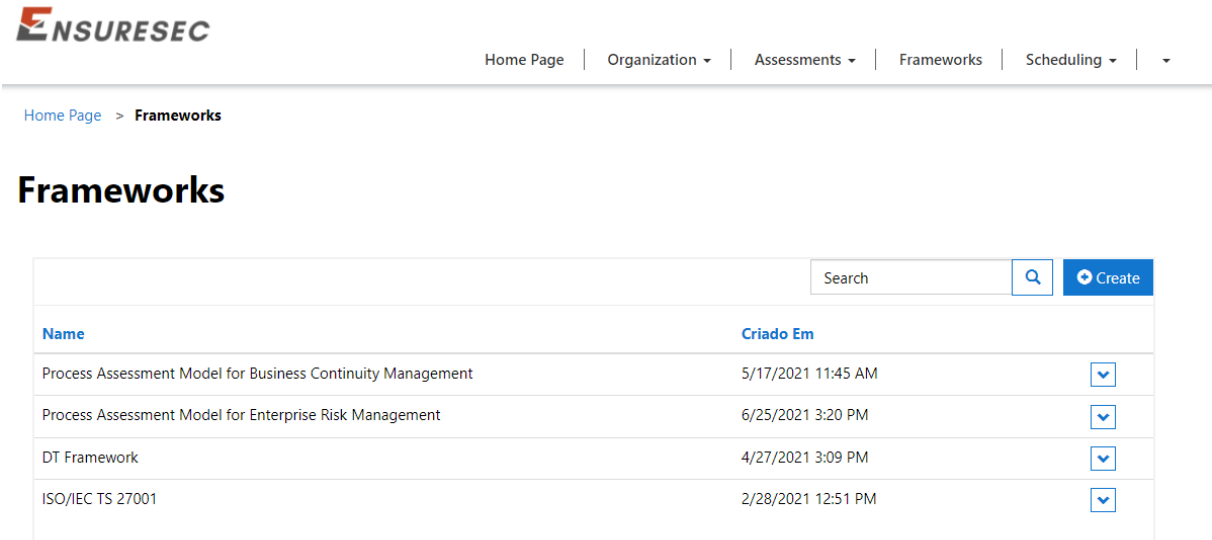


Figure 7.13. List of frameworks added in the application using the insert in bulk functionality

The user can also insert a framework using the front-end, as shown in Figure 7.14. The difference between this and the previous method is that instead of adding all the information in the tables in-bulk, the frameworks; processes; and outcomes need to be inserted one at a time.

## Create Framework

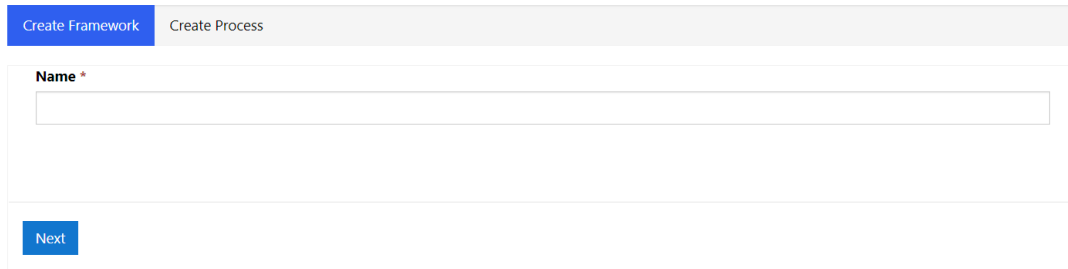


Figure 7.14. Page for inserting a framework using the front-end

## 7.2. Improved Tool

As described and discussed in Sections 8.1 and 8.2 in the next Chapter, the first version of the tool was evaluated during two unstructured interviews and in a field study, where it was used to support and audit.

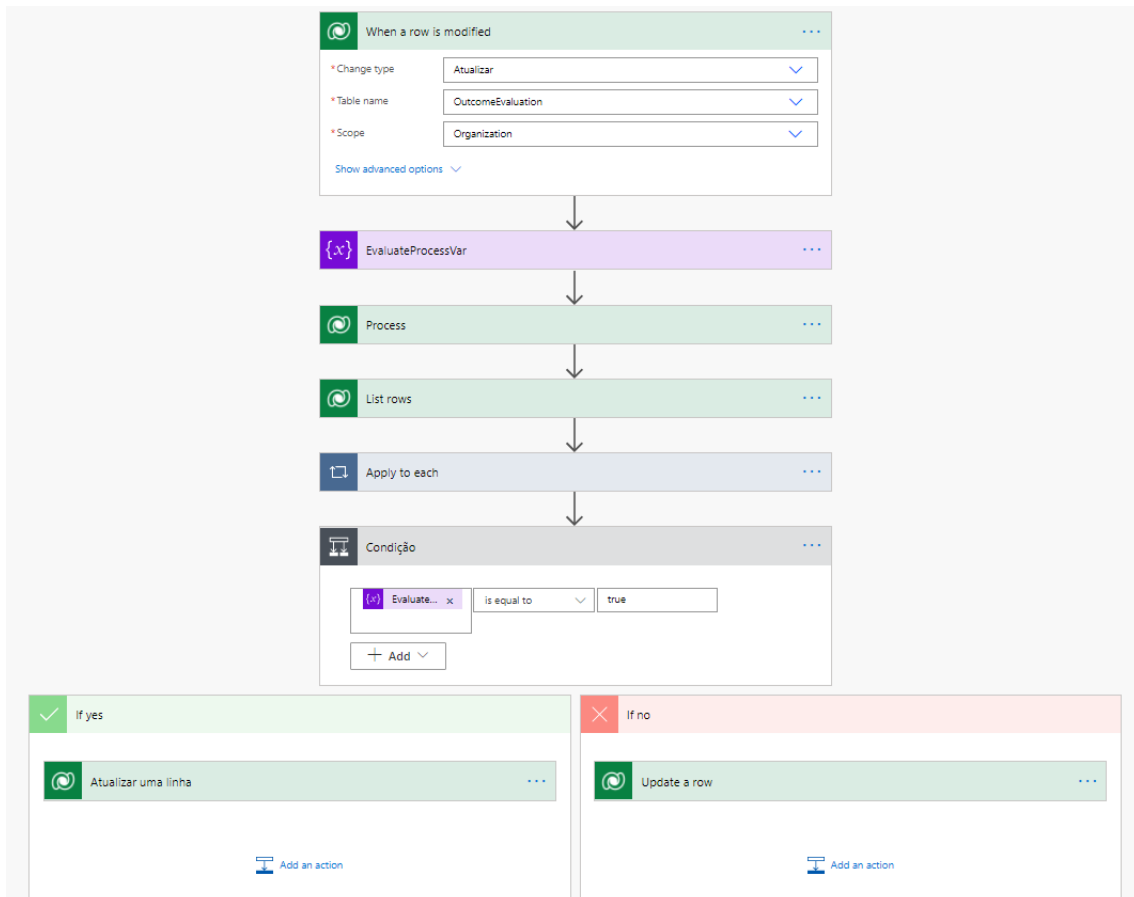
As a result of these evaluation activities, some suggestions were collected to improve the tool. Due to time limitations, we were not able to implement all suggestions. Thus, we considered the improvements that were simple to implement, and two more complex functionalities. In particular, one improvement (described in Section 7.2.2) required some changes to the original model, which are explained in the corresponding section.

### 7.2.1. Automatic Process Rate

The rate of a process is dependent on the rate of its outcomes. Therefore, an algorithm was created to automatically rate a process to level 1 concerning that all outcomes of that process are rated “Partially achieved” or “Largely achieved”. This rating could be updated at any time by the auditor, but would assign an initial value to the process rate given that the described condition is met.

To achieve this, we used Microsoft Power Automate<sup>12</sup>, a technology from the PowerApps Suite that allows to build automated processes based on flows. The flow created for this automation, comprising all the steps executed, is displayed in Figure 7.15.

<sup>12</sup> Microsoft Power Automate: <https://powerautomate.microsoft.com/> (Accessed 19/09/2021)



**Figure 7.15.** Flow for automatically setting the rate of a process when all outcomes are rated as “Partially achieved” or “Largely achieved”.

The first step corresponds to the trigger of the automation: the algorithm will execute *when a row is modified* – more specifically, when a row of the table *Outcome* is modified. Then, step two is *EvaluateProcessVar*, where the system creates a variable with value “True”. This variable will indicate, later on, whether the process rate will be automatically updated or not.

In the third step (*Process*), the system will read the process associated with the outcome that was previously edited, which will be used to list all the outcome evaluations of the process (step four – *List rows*). In the fifth step (*Apply to each*), the system will check, for each record that was listed, if the evaluation of the outcome has a rate different from “Partially achieved” or “Largely achieved”. If this condition is verified, then the variable defined in step 2 is set to false.

On the sixth step, the system checks if the variable created in step two has the value “True” value. If it has, the rate of the process is set to “1”; otherwise the rate of the process will be null.

Regarding the originally proposed model, the activity diagram corresponding to functionality 5 (evaluate process based on the rate of outcomes) and shown in Figure 6.6 is not changed, since the user can always define a rate. However, this improvement defines, in some cases, a default value.

## 7.2.2. Reporting

The reporting functionality was the most mentioned during the phases where the problem was identified and the goals for this research were defined. However, this functionality was not included in the first version of the tool, because the initial focus was on creating the base structure for software tool.

During the interviews that helped validating the initial tool (as described in Section 8.1), both interviewees reinforced the importance of having a reporting functionality. The first interviewee suggested to create reports that summarize a particular assessment, while the participants of the second interview suggested to create benchmark reports to compare the results of an audit to those achieved in other audits in organizations of the same business sector.

The latter type of reports were very challenging to implement using the PowerApps technology, given that the whole structure needed to be revised. Given the time available to perform these improvements, we decided to create only the assessment reports.

Therefore, we added the requirements listed in Table 7.1 to the original model, thus expanding the requirements list in Table 6.2.

**Table 7.1.** Requirements for the reporting functionality

Category	Title	Requirement
Reports	Report of an assessment	The system should allow the users to be able to retrieve a report that has all activities performed on an assessment
	General reports	The system should allow the users to be able to see reports about the general use of the platform (number of assessments made and for which organizations)

The assessment report was created to list all the activities conducted in a specific assessment. For accessing this functionality, the user must access a specific assessment and then click on the button “Final Report”, as shown in Figure 7.16. This will open a new page (shown in Figure 7.17), where all processes and associated outcomes (with the rates assigned) will be listed. The auditor can print this report by clicking on the “Print” button.

The general report, which allows the user to get an overview of his/her general activity in the platform, is displayed in Figure 7.18. The report was built using Microsoft PowerBI<sup>13</sup>, a technology from the PowerApps Suite that allows to create dashboards and reports. The user can see the total number of assessments, and those who were fully or partially conducted. The auditor can also see the number of assessments per business sector in a bar chart.

## 7.2.3. Other improvements

Additionally to the two previous and more complex improvements, other minor changes were performed in the proposal.

---

<sup>13</sup> Microsoft PowerBI: <https://powerbi.microsoft.com/> (Accessed 19/09/2021)

## Edit Assessment

Assessments > Edit Assessment

Final Report

**Assessment \***  
 Teste

**Framework**  
 ISO/IEC TS 27001

**Organization**  
 Organização Alexandre

**Assess full framework? \***  
 No  Yes

**ProcessEvaluation**  
 Open Processes ▾

---

**Process ↑** **Created on**

Asset management	9/9/2021 5:49 PM	▾
------------------	------------------	---

**Figure 7.16.** Assessment page, from where the auditor can access the assessment report by clicking on “Final Report” button (highlighted with a red rectangle)

Print

### Auditoria 27001 27/08

ISO/IEC TS 27001

Organização Alexandre

Process

Name	Rate
Communication management	

Outcomes

Name	Rate	Information

Process

Name	Rate
Documentation management	

Outcomes

Name	Rate	Information

**Figure 7.17.** Assessment report. The auditor can print it by clicking on the “Print” button (highlighted with a red rectangle)

## Global Report



**Figure 7.18.** Report on the tool

The form for creating an organization was updated by including a field for storing the address of the company. Thus, the screen displayed in Figure 7.4 was updated as shown in Figure 7.19.

## Create Organization

Information of Organization

Create Employees

**Name \***

**Business Sector \***

▼

**Address \***

**Figure 7.19.** Form for creating an organization, with the new Address field (highlighted with a red rectangle)

The usability improvements and bugs reported in the field study (as discussed in Section 8.2) were implemented, except for listing the inputs and outputs of an assessment (number 1) and adding more options to the list of business sectors (number 5), which were discarded due to time limitations and because they had a low priority.

In Figure 7.20 we show an example of a usability improvement implemented. Given that inserting an assessment requires a somehow long flow of linked pages to be accessed, a breadcrumb menu was created on the top of the page, which allows the user to jump between pages more easily.

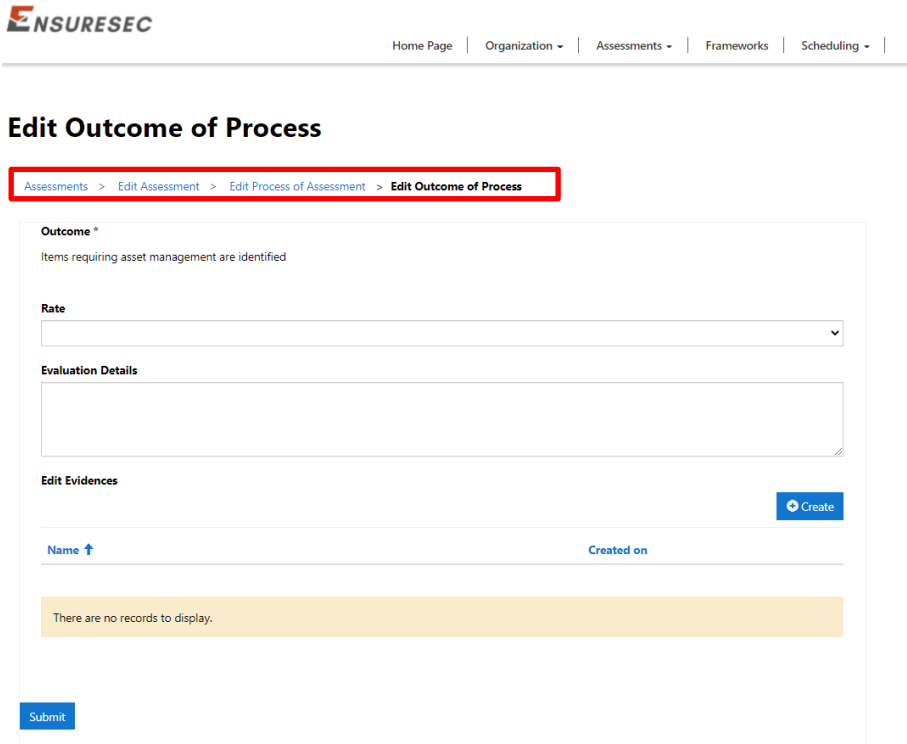


Figure 7.20. Navigation bar on the assessments page improved (highlighted with a red rectangle)



## 8. Evaluation

This Chapter corresponds to the evaluation step of DSR, where we evaluated the outcomes of the demonstration activity and confirm if and how the proposal can be used to address the stated problem.

The proposed artefact was evaluated using qualitative methods, including interviews and a field study. In Section 8.1 we present the two unstructured interviews conducted to evaluate the initial version of the tool, and Section 8.2 reports the results of the field study, where the tool was used in a real-setting. In Section 8.3 we describe the set of semi-structured interviews that were led with experienced auditors to gather information about gaps and possible improvements on the improved tool.

The results of all evaluation activities are discussed in Section 8.4.

### 8.1. Interviews for Tool Validation

The prototype described in Section 7.1 was evaluated in two unstructured interviews, both with the goal of gathering feedback regarding the validity and utility of the tool (and, as a consequence, the underlying model).

The first interview was arranged with one of the experienced auditors that participated in the interviews described in Section 2.1 – more specifically, A1, since he demonstrated interest and availability to provide intercalary feedback during the research work.

Overall, the auditor did not point out any major issue with the model, but two minor improvements and one new functionality were suggested. Regarding the overall concept of rating the assessments (comprising functionalities 5 and 6 from the model proposed), he suggested the creation of an algorithm that could, automatically, rate a process to level 1 if all the outcomes of that process have the rate “Partially achieved” or “Largely achieved”.

As for the creation of an organization (functionality 1 of the model), it was suggested that the form should have an input where the auditor can fill the address. This will allow the auditor to distinguish between different locations of the same organization.

The auditor also reinforced the suggestion made in his first interview (described in Section 2.1) to create a report functionality that could generate reports based on the activity performed during the audit of a particular assessment.

The second interview was conducted with three participants from a partner of the European Project under which this research work was conducted. This partner is a multinational Portuguese organization of the retail area, and the participants were a project manager; an auditor; and the head of security.

As in the first interview, the participants believed that the main functionalities were well implemented and adapted to real-world usage. They also provide some new feedback regarding new functionalities that could be implemented.

It was proposed that the team should create a timeline functionality that could aggregate several assessments to a single process. This could allow the auditors to continuously improve the audited processes between different assessments, and could also create some metrics such as how many audits were performed to achieve a final goal.

Also, it was suggested to create some reports to benchmark audits' results between organizations, i.e. to compare the performance of the audits of one specific organization to other organizations in the same business sector.

## **8.2. Field Study**

The initial tool described in Section 7.1 was also evaluated in a field study, where an audit was performed with support of the developed tool in a multinational organization working on the rental car business area. This audit was based on the digital transformation framework described in Section 7.1.1, and conducted by a master's degree student in the context of her thesis' research work.

After completing the audit, the participant provided feedback regarding its use, so that we could understand the stronger and weaker points of the proposed solution. She said that the audit was performed without facing any major issues. However, several improvements were mentioned that should be implemented in the tool:

1. When visualizing an assessment, make the inputs and outputs visible to the auditor;
2. Order the list of processes of an assessment by rate;
3. Add a filter to the list of processes to allow the auditor to select the ones that were not audited;
4. Add a filter to the list of outcomes to allow the auditor to select the ones that were not audited;
5. Add more options to the list of business sectors.

Moreover, some bugs were reported, which are listed on Table 8.1. Most of these bugs were minor and corresponded to issues with the labels (bugs 4-11), which were either written in Portuguese instead of English, as the remaining of the app (bugs 4-9) or wrong (bugs 10-11). The remaining bugs (1-3) reported usability issues.

## **8.3. Final Interviews with Experts**

The improved tool, which is described in Section 7.2 and refined based on the feedback received and discussed in Sections 8.1 and 8.2, was evaluated based on a set of semi-interviews. The interviewees correspond to the same eight experienced auditors who participated in the interviews described in Section 2.1 for investigating the research problem.

As in the previous set of interviews, these sessions were held remotely (via Zoom), and were recorded (with the permission of the interviewees) and then revised to take notes and organize the results. Interviews were conducted between June and September 2021, and took between 45 minutes and one hour.

**Table 8.1.** Bugs reported during the field study

<b>ID</b>	<b>Title</b>	<b>Description</b>
1	Navigation buttons on the page “Evaluate process” and “Evaluate outcome”	The pages “Evaluate process” and “Evaluate outcomes” should have buttons that allow the user to navigate between the processes of an assessment and the outcomes.
2	Add number to outcomes	Each outcome should have a field called “Number” where the number of the outcomes is stored.
3	Order of Outcomes	The outcomes of a process of an assessment should be ordered by its number.
4	Labels in “Evaluate assessments” page not written in English	Some of the labels of the page are in Portuguese.
5	Columns names of table “Scheduling” not written in English	The columns of the table “Scheduling” should be written in English
6	Labels on the Add Employees’ page not written in English	When a user tries to add an employee to an organization, the labels in that page should be written in English and not in Portuguese
7	Success Message not written in English	Success Message should be written in English
8	Labels on the Profile page not written in English	All the labels of the page “profile” should be written in English
9	Labels on the Organization page not written in English	Some of the labels of the page “Organization details” should be translated to English
10	Labels on the “Edit Assessment” page are wrong	Label “edit” should be “Evaluate”, and label “name” should be process
11	Labels on the “Edit outcome” page are wrong	Label “Edit Outcome” should be “Evaluate Outcome”, and label “Name” should be “Outcome”.

During the interview, the improved tool was demonstrated, and for each feature the same three questions were posed to the interviewees:

- Do you think that this functionality can help improving the auditing process?
- Does this functionality pose any limitation?
- Do you have any suggestion on how to improve this functionality?

In the end, the interviewees were asked whether they had additional suggestions for improving the tool. Because we already had interviewed all participants, there were no questions regarding the interviewees’ profile, which can be consulted in Section 2.1.

All interviewees agreed that the proposal was overall good for an initial version of the tool, and would be helpful in clarifying and structuring the audit process. Nevertheless, the auditors proposed some improvements to the tool, mostly to address identified limitations. These improvements can be found in Table 8.2 (categorized by functionality).

**Table 8.2.** Improvements suggested by the interviewees

	A1	A2	A3	A4	A5	A6	A7	A8
<b>1. Create organization and associate employees</b>								
Add a field for indicating the organization's size			X				X	X
Add more fields for employee information (e.g. his/her projects)					X	X		
Integrate the tool with the user management system Azure AD				X				
Replace the address field with a list of districts							X	
<b>3. Creation of a new assessment</b>								
Associate relevant stakeholders to the processes	X	X						
Add more information about the audit					X		X	
Indicate the areas of the organization that are being audited	X				X			
Indicate the physical sites where the audit was conducted	X							
Replace the label "Assess Entire Framework" with "Scope"							X	
<b>4. Add evidence to an outcome</b>								
Associate one evidence to multiple outcomes		X	X					
<b>9. Reporting</b>								
Add fields for the auditor to write a general evaluation of the audit	X	X	X	X	X	X	X	X
Create different reports for different stakeholders			X			X	X	X
<b>Other</b>								
Include multiple frameworks in one audit							X	
Add the ability to include standards in the tool							X	
Organization should be able to submit information							X	
Automated workflows to validate simpler requirements							X	

Regarding the creation of an organization, three auditors suggested to include a field to indicate the size of the organization being created. Moreover, A5 and A6 stated that there are few fields for providing employee information (such as his/her projects and main responsibilities), since department and role are not enough to categorize an employee.

Moreover, A4 suggested to integrate the application with Azure Active Directory<sup>14</sup> (AD) is a limitation, given that all software is part of the Power Platform stack. Finally, A7 suggested to replace the Address field with a list of districts for the user to select from, which would help when computing statistics.

When creating an assessment, A1 and A2 suggested that it should be possible to associate the relevant stakeholders to the processes, including people whose work is being audited; top managers that want to receive the results, etc.

A5 and A7 stated that more information should be added regarding the audited, such as the start and end dates. More specifically, A1 and A5 suggested that it should be possible to indicate the areas of the organization and are being audited (e.g. IT, Human Resources; etc.), while A1 also mentioned that physical sites could also be subject to an audit.

When adding evidences to an outcome, A2 and A3 suggested that it should be possible that one evidence could be linked to many outcomes.

Concerning the reporting functionality, all auditors agreed that it should be possible for the auditor to submit a general remark/evaluation of the audit. Furthermore, A1, A2, A3, and A4 further indicated that having a single field for final conclusions would be enough to address this.

<sup>14</sup> **Azure Active Directory:** <https://azure.microsoft.com/en-us/services/active-directory/> (Accessed: 27/09/2021)

Additionally, four auditors further suggested to create different reports for different stakeholders involved in the audits. For example, the top managers might need to have a report based on graphs and with more direct and concise information. On the other hand, the technical roles would be more interested in the reports already generated by the tool, since it contains more detailed information regarding the technical details of the audit.

Regarding the remaining functionalities (meetings schedule; evaluate processes and outcomes; and inserting frameworks), no limitations or improvements were discussed.

Additionally to the already existent functionalities, A7 suggested the creation of new functionalities. He suggested that it should be possible to cover multiple frameworks in one audit, since it is usual to conduct an audit focused on more than one framework.

A7 further suggested to add the possibility to include not only maturity models, but also the standards itself. For example, instead of being able to add the ISO/IEC 27001 maturity model, it should be possible to directly add the ISO/IEC 27001 standard.

Finally, A7 suggested a more advanced feature, where it would be possible for the organization to submit most of the information through the application, so that the auditor would have information organized beforehand. In some cases, the software tool could have automated workflows to validate some simpler requirements.

Finally, an interesting output of these interviews is that, when we asked if it would be possible for them to use the tool in a real audit, they all mentioned that they never used, or had any knowledge of it being used, a maturity model based on the ISO/IEC 330xx structured approach. This means that, while they were available to test the application, they could not do it unless it supported another standard structure.

Consequently, we had no opportunity to test this application in a real-world scenario.

## **8.4. Discussion**

The goal of this research was to create a proof of concept tool to validate whether a software tool could be helpful in assisting an auditor to determine the capability of a process in a concise and efficient way. Overall, and based on the feedback collected during the three evaluation activities, the software tool has the potential to help address the defined research problem, although several improvements are needed.

We found that the reporting functionality, which was the most mentioned during the whole research work, is really essential in such a tool. While it was not included in the initial version of the tool, we added some reporting tools in the improved version. In the future, this must be improved, for example by creating specific reports for different roles, and benchmark reports to compare the results of the audit with those of organizations in the same business sector.

Moreover, there is much information that the tool should be collecting regarding the organization (e.g. its size); its employees (e.g. his/her projects and main responsibilities); and the audit itself (e.g. areas

of the organization or physical site being audited). We also found important to associate stakeholders with the processes, something that was already mentioned in the initial interviews (described in Section 2.1) but not implemented during this research.

An important conclusion that had a major impact in this research work is that the ISO/IEC 330xx structured approach does not seem to be used in the real-world organizations. This means that, although the tool is generic enough to support any framework based on this structure, we could not demonstrate the proposal in a real-world audit. Therefore, it is important that, in the future, the tool can support standards or maturity models that are more used in the industry.

Nevertheless, while the tool was indeed demonstrated during an audit, this audit was conducted by a master degree student, and not by an experienced auditor. This is reflected on the feedback received, which was mostly focused on usability issues. While this was important to improve the overall quality of the tool, it was not enough to understand what could be done to improve the audit process.

To summarize, the proposed tool seems to be helpful in addressing the research problem, because it indeed allows to create a structured approach to collect and evaluate evidence during audits, by making the outputs more transparent and providing means for a more efficient audit process. However, the feedback collected suggests that the ability to determine the capability of a process does not seem to be very useful, namely for this maturity model structure. The tool is still in a very initial stage, and thus requires more iterations of design and evaluation. However, this initial version seems to have potential to become a useful tool in the future.

## 9. Conclusion

In this final chapter, we provide a summary of the work performed during this research.

Audit processes can be useful for organizations to better understand the capability of their organizational processes and define strategies for their continuous improvement. Nevertheless, these activities are often subject to some challenges, given their bureaucratic and manual nature.

In this research work, we followed a DSR methodology to better understand the problem; define goals for a solution; and produce an artifact that could help addressing the identified problem.

First, it was important to understand the current state of the art in the field. To accomplish this, we conducted a set of interviews with experienced auditors to collect insights regarding their work; the main challenges they face; and how they could be addressed. Then, we studied some compliance software tools to understand their characteristics and gaps.

Finally, this work was complemented by conducting a SLR to understand whether the topic has been address by other researchers. More specifically, we tried to understand how a software tool can help organizing and optimizing the auditors' work, and which are the characteristic of the tools proposed in the selected studies. We found that, while there is interest in this subject, the research is still preliminary.

Therefore, we believed that this was a good investigation opportunity. Based on the results collected during the interviews; the theoretical background analysis; the commercial tools' analysis; and the literature review; we defined the boundaries of this research and the characteristics of the artefact proposed.

We developed a model for a software tool that follows the structure proposed in the ISO/IEC 330xx family of standards, so that it would be generic enough to support different frameworks. This model comprises a set of functionalities; its requirements; an UML diagram; and an activity diagram for each functionality.

Then, the model was instantiated in a prototype, which was validated in a set of interviews with experts and by a field study with a master degree student. Based on this feedback, the tool was improved by addressing some minor usability issues and by implementing two additional features.

Finally, the improved version was evaluated during a set of interviews with the same auditors interviewed during the problem investigation. Overall, the feedback was fairly positive, since the auditors did not find any major issue with the tool. However, it is still in a very initial stage, since more information should be collected and other functionalities, such as the reporting, should be subject to major improvements.

In the following sections, we discuss more in-depth the main lessons learned during this research work; its most important contributions and limitations; and some research lines for future work.

## 9.1. Lessons Learned

In this Section, we present and discuss the main lessons learnt during this research.

- While being a novel subject, there seems to be some interest in using software tools to improve the efficiency and transparency of the audit's process, as we found mainly during the interviews and the literature review.
- While it was not possible to evaluate the tool in a real assessment, by a real auditor, the feedback gathered suggests that using a software tool to support the audit process seems to have a positive impact on the auditors' work, as it allows to gather evidences; create reports; and maintain the history of audits and audit information in a more organized; concise; and efficient way.
- Nevertheless, this potential could only be unleashed by generalizing the tool to support standards that are not based on maturity models following the structure proposed in the ISO/IEC 330xx family of standards.

## 9.2. Contributions

This research provided the following contributions:

- **The research conducted to study and define the research problem**, which included a triangulation of the results of a set of interviews with experts and a literature review on the topic.
- **The research conducted regarding the use of software tools to support the audit processes**, which included a literature review and an analysis of some already existent tools.
- **The model of a software tool to help assessors determine the capability of a process in a structured and efficient way**, which was developed based on the outputs of the two previous contributions. This model was created by following a structured and detailed process, which started by selecting the list of features and their requirements; then creating the UML diagram; and finally the set of activity diagrams describing the flow of the the selected functionalities.
- **The software tool developed**, which is an instantiation of the previous model. This tool was developed as a web application, where two frameworks were loaded.
- **A preliminary evaluation of the tool**, based on a set of interviews with experts and a field study with a master student, which allowed to validate the concept and to collect important improvements suggestion for the tool.

Additionally, this research was communicated to relevant audiences. An article was produced and submitted to Digital Policy, Regulation and Governance (rank Q2), a journal that is relevant to the research field we are working on. This paper summarizes the research presented in this document and present the results obtained by demonstrating and evaluating the proposal.

This dissertation report and its presentation and discussion with a qualified jury are also a means for communicating this work. Moreover, this research work was presented in two formal meetings of the



H2020 ENSURESEC project. While no formal feedback was collected, these meetings allowed us to communicate the results to all of the involved entities in this European project.

### **9.3. Limitations**

This research work poses some limitations that should be acknowledged.

While we were only able to conduct eight interviews with experienced auditors, we believed that we have reached saturation in the feedback collected. However, we cannot guarantee that these results can be generalized to all auditors. To address this, we tried to describe the interviewees' profile to contextualize their opinion.

The commercial tools' analysis was not fully systematic, thus there is the risk that some relevant compliance software tool might have been left out the analysis.

Not all of the identified functionalities and suggested improvements could be implemented, and thus evaluated. Thus, not all of the functionalities that are important to support the auditors' work could be integrated in the tool. These aspects are further discussed in Section 9.4 while discussing venues for future work.

While the tool was used during a real audit, it was conducted by a master student, with no previous experience as an auditor. This is evident in the feedback received, which was mostly focused on usability issues, which despite relevant are not the main focus of an experienced auditor.

However, the tool could not be evaluated by an experienced auditor, in a real organization, because, as we already discussed, the structure of the tool (based on the ISO/IEC 330xx family of standards) is not used in the industry.

### **9.4. Future Work**

There are some potential directions to improve and extend this research work in the future.

There were many features and improvements to the software tool discussed throughout this research that we had no opportunity to implement since it would require a significant implementation effort. Adding the possibility to create forms to gather evidence without the need to run meetings would help improving the efficiency of the audit processes. Moreover, it would be interesting to integrate the tool with the Azure AD user management, and to add the possibility to define the processes' stakeholders.

Additionally, there are other more advanced features that would be only possible to implement when the software tool is in a more mature stage. These features would also require major changes to the model proposed.

One of those features is the support to continuous improvement, which would allow to associate multiple assessments in a single work package, thus keeping track of results between different audits of the same area/subject.

Another example is the possibility to benchmark audit results between organizations of the same business sector, which would help organizations compare their results with those of similar organizations. In this line, the reporting tools can also be improved, including the creation of different reports in the tool.

Finally, an important venue for future work is to change the model of the proposal to support other standards that are not based on the maturity model structure defined by the family of standards ISO/IEC 330xx. This would make it easier to find organizations where the tool could be used by an experienced auditor during a real-world audit process.

This would allow for more accurate results, and to consider other aspects that could not be evaluated during this research, such as the duration of the assessments while using the artefact and the relative effort needed to use the solution (including the configuration, insertion, and analysis activities). Additionally, it would be possible to analyse the logs produced by the software tool to study aspects such as the number and type of evidences updated.

# Bibliography

- [1] O. Rasit Yurum, Ö. Özcan-Top, and O. Demirörs, "Assessing Software Processes over a New Generic Software Process Assessment Tool," *Roczniki Kolegium Analiz Ekonomicznych/Szkoła Główna Handlowa*, vol. 43, no. 7--29, 2016.
- [2] "CMMI Product team: CMMI for Development (CMMI-DEV). Version 1.3. Technical Report, CMU/SEI-2010-TR-033," 2010.
- [3] Office of Government Commerce, *ITIL: Continual Service Improvement*. Norwich, UK: The Stationary Office, 2011.
- [4] "International Organization for Standardization."
- [5] "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements," 2013.
- [6] "ISO 9001:2015 Quality management systems — Requirements," 2015.
- [7] J. L. Barthelemy and M. Zairi, "Making ISO 9000 work: the role of auditing," *Measuring Business Excellence*, 2000.
- [8] Office of Government Commerce, *ITIL: Continual Service Improvement*. Norwich, UK: The Stationary Office, 2011.
- [9] V. H. Haase, "Software process assessment concepts," *Journal of Systems Architecture*, vol. 42, no. 8, pp. 621--631, 1996.
- [10] T. J. Crowe, J. S. Noble, and J. S. Machimada, "Multi-attribute analysis of ISO 9000 registration using AHP," *International Journal of Quality & Reliability Management*, 1998.
- [11] K. Peffers, T. Tuunanen, M. a. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45--77, 2008, doi: 10.2753/MIS0742-122240302.
- [12] O. Rasit Yurum, Ö. Özcan-Top, and O. Demirörs, "Assessing Software Processes over a New Generic Software Process Assessment Tool," *Roczniki Kolegium Analiz Ekonomicznych/Szkoła Główna Handlowa*, vol. 43, no. 7--29, 2016.
- [13] A. Shrestha, A. Cater-Steel, M. Toleman, and W.-G. Tan, "Building a Software Tool for Transparent and Efficient Process Assessments in IT Service Management," in *International Conference on Design Science Research in Information Systems*, 2014, pp. 241--256.
- [14] V. H. Haase, "Software process assessment concepts," *Journal of Systems Architecture*, vol. 42, no. 8, pp. 621--631, 1996.

- [15] A. Shrestha, A. Cater-Steel, M. Toleman, and W.-G. Tan, "Building a Software Tool for Transparent and Efficient Process Assessments in IT Service Management," in *International Conference on Design Science Research in Information Systems*, 2014, pp. 241--256.
- [16] M. E. Fayad and M. Laitnen, "Process assessment considered wasteful," *Communications of the ACM*, vol. 40, no. 11, pp. 125--128, 1997.
- [17] M. Staples, M. Niazi, R. Jeffery, A. Abrahams, P. Byatt, and R. Murphy, "An exploratory study of why organizations do not adopt CMMI," *Journal of Systems and Software*, vol. 80, no. 6, pp. 883--895, 2007, doi: 10.1016/j.jss.2006.09.008.
- [18] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," 2007. doi: 10.1145/1134285.1134500.
- [19] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," 2007. doi: 10.1145/1134285.1134500.
- [20] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS quarterly*, vol. 28, no. 1, pp. 75--105, 2004.
- [21] K. Peffers, T. Tuunanen, M. a. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45--77, 2008, doi: 10.2753/MIS0742-1222240302.
- [22] J. E. Van Aken, "Management research as a design science: Articulating the research products of mode 2 knowledge production in management," *British Journal of Management*, vol. 16, no. 1, pp. 19--36, 2005, doi: 10.1111/j.1467-8551.2005.00437.x.
- [23] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS quarterly*, vol. 28, no. 1, pp. 75--105, 2004.
- [24] H. Alan and C. Samir, "Design Science Research in Information Systems," *Design Research in Information Systems. Integrated Series in Information Systems*, vol. 22, 2010, doi: [https://doi.org/10.1007/978-1-4419-5653-8\\_2](https://doi.org/10.1007/978-1-4419-5653-8_2).
- [25] T. Phan, L. Lai, T. Le, and D. Tran, "The impact of audit quality on performance of enterprises listed on Hanoi Stock Exchange," *Management Science Letters*, vol. 10, no. 1, pp. 217--224, 2020.
- [26] A. Twycross and A. Shorten, "Service evaluation, audit and research: what is the difference?," *Evidence-based nursing*, vol. 17, no. 3, pp. 65--66, 2014.
- [27] "Standards," *ISO*. Jun. 2020.
- [28] "International Organization for Standardization."
- [29] J. T. Hackos, "International standards for information development and content management," *IEEE Transactions on Professional Communication*, vol. 59, no. 1, pp. 24--36, 2016.

- [30] S. Marshall, "A Quality Framework for Continuous Improvement of E-Learning: The E-Learning Maturity Model.," *Journal of Distance Education*, vol. 24, no. 1, pp. 143–166, 2010.
- [31] "ISO/IEC 33002:2015," *ISO*. Jun. 2020.
- [32] C. Svensson and H.-H. Hvolby, "Establishing a business process reference model for Universities," *Procedia Technology*, vol. 5, pp. 635–642, 2012.
- [33] T. Varkoi, "Process assessment in very small entities-An ISO/IEC 29110 based method," in *2010 Seventh International Conference on the Quality of Information and Communications Technology*, 2010, pp. 436–440.
- [34] "ISO/IEC TS 33052:2016," *ISO*. Jun. 2020.
- [35] "ISO/IEC TS 33072:2016," *ISO*. 2016.
- [36] "ISO/IEC 27001 - Information security management," *ISO*. 2020.
- [37] C. Wohlin, P. Runeson, M. Höst, M. C. Ohlsson, B. Regnell, and A. Wesslén, *Experimentation in Software Engineering*. Springer Science & Business Media, 2012.
- [38] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS quarterly*, 2002.
- [39] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," *ACM International Conference Proceeding Series*, 2014, doi: 10.1145/2601248.2601268.
- [40] R. Wieringa, N. Maiden, N. Mead, and C. Rolland, "Requirements engineering paper classification and evaluation criteria: a proposal and a discussion," *Requirements engineering*, vol. 11, no. 1, pp. 102–107, 2006.
- [41] "ISO/IEC TS 33052:2016," *ISO*. Jun. 2020.
- [42] "ISO/IEC TS 33072:2016," *ISO*. 2016.