INSTITUTO
UNIVERSITÁRIO
DE LISBOA

RPA for Efficient Compliance Screening

Mamasaliu Djau

Master in Digital Technologies for Business

Supervisors:

Professor Doctor Rúben Filipe Pereira, Assistant Professor,
ISCTE – Instituto Universitário de Lisboa

Master Engineer Fábio Sousa,
Siemens

December, 2024

TECNOLOGIAS
E ARQUITETURA

RPA for Efficient Compliance Screening

Mamasaliu Djau

Master in Digital Technologies for Business

Supervisors:

Professor Doctor Rúben Filipe Pereira, Assistant Professor,
ISCTE – Instituto Universitário de Lisboa

Master Engineer Fábio Sousa,
Siemens

December, 2024

Dedicated to Bárbara Rosa and Rui Oliveira Marques,

for their commitment to promoting human rights,

democracy and civic engagement.

Acknowledgment

I would like to express my deepest and sincerest gratitude to Professor Rúben Pereira and Fábio Sousa for their guidance and tireless support in creating this thesis and developing the POC. I would also like to thank my classmates and the professors for sharing knowledge and creating a stimulating environment, and the ISCTE teams for their constant availability and support.

Resumo

Este trabalho explora a aplicação da *Robotic Process Automation (RPA)* em *compliance*, especificamente no contexto de combate à lavagem de dinheiro e combate ao financiamento do terrorismo. Investiga-se como a RPA pode automatizar a extração, compilação, harmonização de listas de sanções emitidas por organizações internacionais e conduzir a verificação de nomes. O estudo demonstra as melhorias de eficiência e precisão obtidas através de uma *Proof-of-concept (POC)*, destacando o potencial da RPA para dar eficiência a processos de *compliance*, reduzir custos operacionais e melhorar a aderência regulatória.

Palavras-chave: RPA; Conformidade; Prevenção à Lavagem de Dinheiro; Sanções; Automação.

Abstract

This thesis explores the application of Robotic Process Automation (RPA) in compliance screening, specifically within the context of anti-money laundering (AML) and counter-terrorist financing (CTF). It investigates how RPA can automate the extraction, compilation, harmonization of sanctions lists issued by international organizations and conduct screening of names. The study demonstrates the efficiency and accuracy improvements achieved through a Proof of Concept (POC), highlighting RPA's potential to consolidate compliance processes, reduce operational costs, and improve regulatory adherence.

Keywords: RPA; Compliance; Anti-Money Laundering; Sanctions; Automation.

Index

Index of Figures

Index of Tables

List of Acronyms

Acronym	Meaning
AI	Artificial Intelligence
AML	Anti-Money Laundering
API	Application Programming Interface
CDD	Customer Due Diligence
CRM	Customer Relationship Management
CTF	Counter-Terrorist Financing
DSR	Design Science Research
ERP	Enterprise Resource Planning
EU	European Union
FATF	Financial Action Task Force
GDPR	General Data Protection Regulation
IMF	International Monetary Fund
IPA	Intelligent Process Automation
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
KPI	Key Performance Indicator
ML	Machine Learning
NLP	Natural Language Processing

POC	Proof of Concept
RBA	Risk-based Approach
ROI	Return on Investment
RPA	Robotic Process Automation
RegTech	Regulatory Technology
WB	World Bank
UML	Unified Modelling Language
UN	United Nations

CHAPTER 1

Introduction

In the contemporary business environment, compliance with national and international regulations is fundamental, particularly in anti-money laundering (AML) and counter-terrorist financing (CTF). Organizations must adhere to various sanctions lists issued by international bodies such as the United Nations (UN), the European Union (EU), and individual countries to mitigate the risks associated with economic and financial crimes. The European Commission's Third Directive on AML mandates a risk-based approach (RBA) to AML regulation, focusing on optimizing resource allocation toward the highest risks, enhancing the effectiveness of AML measures [1], this emphasizes the need for financial institutions to design adaptive controls, aiming to increase the detection of accurate suspicious transactions while balancing economic and reputational costs.

Economic sanctions are a standard and powerful instrument in international politics and economic relations, employed predominantly by countries such as the United States and multilateral organizations, including the UN. These sanctions are imposed on target countries, individuals, or organizations with the intent of exerting economic pressure to alter their behaviour potentially [2]. By restricting access to financial markets, freezing assets, and prohibiting trade, sanctions aim to compel compliance with international laws and norms, discourage undesirable activities, and promote policy changes within the targeted entities. The effectiveness of these economic sanctions lies in their ability to inflict economic harm, thereby incentivizing the targeted entities to modify their actions to avoid further financial detriment and isolation from the global community [3].

Robotic Process Automation (RPA) has emerged as a transformative technology capable of enhancing business process efficiency by automating repetitive and rule-based tasks without altering existing Information Technologies (IT) infrastructure; it is widely adopted in several sectors [4].

Traditional compliance screening methods typically involve manual processes that are error-prone and resource-intensive. The increasing volume and complexity of regulations require efficient compliance mechanisms, as manual compliance processes are time-consuming and costly, often requiring significant human resources [5]. Businesses' main challenge is accurately identifying individuals or entities on sanctions lists to ensure compliance without high operational costs.

Therefore, to address the challenges in compliance screening, particularly those related to managing sanctions lists, this research aims to achieve one primary objective: develop a proof-of-concept (POC) system that can automate the extraction, compilation, and harmonization of financial sanctions lists. This system will allow compliance screening with accuracy and efficiency, potentially reducing the time and resources required for this task.

This research employs a Design Science Research (DSR) methodology to achieve the objective. DSR is a problem-solving paradigm that seeks to create and evaluate artifacts to solve identified organizational problems. This methodology is particularly suitable for this research as it emphasizes creating and assessing innovative IT artifacts [6]-such as the RPA-based compliance solution-ensuring they effectively address practical problems while contributing to theoretical knowledge. The iterative nature of DSR allows for continuous refinement and validation of the POC, ensuring its relevance and utility in real-world business contexts.

This thesis is organized into five main chapters, each building on the previous one to explore RPA in compliance screening for AML and CTF.

Chapter 1: Introduction

This chapter sets the stage by presenting the background and context of the study. It outlines the growing need for efficient compliance mechanisms in business, particularly in response to complex and evolving regulatory requirements. The chapter also defines the research problem, objectives, and the scope of the study and provides an overview of the selected methodology.

Chapter 2: Literature Review

The literature review offers an in-depth analysis of existing research on compliance screening, the challenges organizations face, and the potential role of RPA as a transformative technology in this context. It highlights key studies on AML and CTF regulations, the limitations of traditional compliance methods, and the current trends in automating compliance processes. This chapter also identifies gaps in the existing research, which this thesis aims to address.

Chapter 3: Research Methodology

This chapter discusses the methodology employed in this study and describes how it was applied to develop and refine the POC system.

Chapter 4: Proof of Concept and Evaluation

The core of the thesis, this chapter outlines the development of the RPA-based compliance screening system. It includes a detailed description of the system design, architecture, and workflow, as well as the prototype development process and the evaluation procedure.

Chapter 5: Conclusion, Limitations, and Future Work

The final chapter summarizes the main findings of the research, highlighting the contributions of the developed RPA solution to optimize compliance screening processes. It discusses the limitations encountered during the study and concludes with recommendations for future research.

CHAPTER 2

Literature Review

This literature review provides an overview of the existing research on compliance screening, specifically focusing on the application of RPA in compliance, particularly for AML and CTF. This chapter discusses the current state of compliance screening processes, the challenges faced by businesses, and the potential of RPA to address these challenges.

The literature review for this thesis involved a comprehensive search of scientific databases, including Scopus, Google Scholar, and IEEE Xplore, to identify relevant academic articles that align with the study's scope and objective. These databases were chosen for their extensive collections of peer-reviewed research in fields related to compliance, AML, CTF, and RPA.

The search process focused on selecting articles that provide theoretical foundations, recent advancements, and practical insights into the use of RPA in compliance screening. 23 articles were selected and thoroughly analyzed to inform the development and evaluation of the RPA-based compliance solution presented in this thesis.

Table 1 summarizes the most relevant articles, highlighting key contributions that significantly influenced the direction and findings of this research. These articles were chosen based on their direct relevance to the core topics of the thesis.

Table 1- Summary of the most relevant articles

Title of the Article	Year	Author	Short Summary
An Investigation into Data Mining Approaches for Anti-Money Laundering	2009	Nhien-An Le-Khac et al.	Explores data mining techniques for anti-money laundering, focusing on identifying suspicious financial patterns through analysis of large datasets.
Anti-Money Laundering by International Institutions: A Preliminary Assessment	2007	Marco Arnone and Pier Carlo Padoan	Assesses the effectiveness of AML/CFT programs by international bodies, highlighting strengths in repressive measures and gaps in preventive actions.
Counter Terrorism Finance by Detecting Money Laundering Hidden Networks Using Unsupervised Machine Learning Algorithm	2020	Amr Ehab Muhammed Shokry et al.	Proposes an unsupervised machine learning model to detect hidden patterns in financial data related to money laundering, aiding counter-terrorism finance efforts.
Introduction to Design Science Research	2020	Jan vom Brocke, Alan Hevner, Alexander Maedche	Provides an overview of the Design Science Research (DSR) methodology, explaining its principles and applications for solving complex problems.
Reporting on the Development of a Web-Based Prototype Dashboard for Construction Design Managers	2024	Barry Gledson et al.	Discusses the creation of a web-based dashboard using DSR methodology to enhance design coordination and performance monitoring in construction projects.
Development of Evaluation Criteria for Robotic Process Automation (RPA) Solution Selection	2023	Seung-Hee Kim	Develops a set of standardized criteria for evaluating RPA solutions, aiming to assist organizations in selecting the right

			tools for business process automation.
Generic Solution Architecture Design of Regulatory Technology (RegTech)	2023	Benny Firmansyah, Arry Akhmad Arman	Proposes a generic architecture for RegTech solutions using RPA, AI, and cloud computing, focusing on automating compliance processes across industries.
Sustainable Implementation of Robotic Process Automation Based on a Multi-Objective Mathematical Model	2023	Leonel Patrício, Lino Costa, Leonilde Varela, Paulo Ávila	Presents a multi-objective model for sustainable RPA implementation, balancing cost efficiency and stakeholder needs.
The Trends and Roles of Robotic Process Automation Technology in Digital Transformation: A Literature Review	2022	Nunik Afriliana, Arief Ramadhan	Provides a literature review on RPA trends in digital transformation, identifying best practices and key success factors for RPA adoption.
Using Design Science Research to Develop Client-Oriented Solutions	2024	Weggeman, L. Cauffman	Demonstrates the application of DSR in creating client-oriented solutions, focusing on iterative design and real-world problem-solving.

2.1. Compliance Screening in Business

Compliance screening is critical for businesses to ensure adherence to various regulatory requirements, particularly those related to AML and CTF. The primary goal of compliance screening is to identify and mitigate risks associated with financial crimes by ensuring that individuals and entities involved in transactions are not listed on international sanctions lists. The AML system imposes significant costs on governments, financial institutions, and customers, including operational expenses, compliance infrastructure, and indirect costs such as inconvenience to customers [7].Traditional compliance methods involve significant manual effort, which can be both time-consuming and prone to human error [8].

In the article "'It could have been us': Peer responses to money-laundering violations in the Dutch banking industry," Anna Merz explores the reactions of Dutch banks to AML violations within their industry. The study identifies six stages of peer interactions—panic and fear, comparing practices, distancing, investing, cooperation, and defiance—that collectively serve as mechanisms for reputation defense and industry-wide response to regulatory scrutiny. Through interviews and content analysis, Merz highlights how banks balance competition with cooperation to optimize AML efforts and navigate public scrutiny, emphasizing the importance of both defensive and collaborative strategies in maintaining compliance and protecting reputational integrity.

2.2. Challenges in Compliance Screening

One significant challenge in compliance screening is the sheer volume of data that needs to be processed and requires businesses to constantly update their internal controls and processes [9], and continuously monitor multiple sanctions lists issued by various international organizations, such as the UN, the EU, and individual countries. These lists are dynamic, with frequent updates and additions, further complicating the screening process.

In today's business, institutions handle enormous amounts of transaction data, making it difficult to manually monitor and identify suspicious activities. Access to realistic, comprehensive datasets for verification and validation [10] is another challenge in compliance screening. Additionally, as highlighted by Ilaria Zavoli and Colin King in their article "The Challenges of Implementing Anti-Money Laundering Regulation: An Empirical Analysis," there are considerable difficulties faced in conducting customer due diligence (CDD), particularly in verifying the identities and sources of funds for clients from foreign jurisdictions.

The complexity of these tasks is compounded by the need to balance thorough checks with maintaining client relationships [11].

2.3. Robotic Process Automation (RPA)

RPA has emerged as a powerful technology capable of automating repetitive and rule-based tasks that humans traditionally perform. It mimics human action and automates routine and repetitive tasks using software robots, providing advantages in terms of cost savings, productivity, error reduction, scalability, non-intrusive implementation, security, ease of use, and overall process efficiency [8].

The article "The Trends and Roles of Robotic Process Automation" by Nunik Afriliana and Arief Ramadhan provides a literature review on the role of RPA in digital transformation. Utilizing a systematic approach, the study analyzes 42 relevant pieces of literature to identify critical trends and applications of RPA across various industries. The findings highlight that RPA significantly improves business process efficiency by automating repetitive and rule-based tasks without altering existing IT infrastructure. It is widely adopted in financial services, banking, and accounting sectors.

The study also identifies critical success factors for RPA implementation, including well-defined processes and strong leadership support, while suggesting that future research should focus on integrating AI and machine learning to tackle more complex tasks [4].

2.4. Application of RPA in Compliance Screening

Applying RPA in compliance screening can offer several advantages, including increased efficiency, accuracy, and consistency. By automating the extraction and verification processes, RPA can significantly reduce the time and effort required for compliance screening, allowing businesses to respond more quickly to changes in sanctions lists, reduce costs, increase process speed, and reduce errors and it is particularly suitable for high-volume, standardized tasks [12].

Moreover, RPA can help minimize human errors, ensuring accuracy in identifying individuals and entities on sanctions lists.

RPA ensures that compliance tasks are performed consistently according to predefined rules, reducing the variability inherent in humans and can generate audit trails and reports, ensuring that all activities are documented and easily retrievable for compliance audits [12].

Benny Firmansyah and Arry Akhmad Arman [5] presents a framework for RegTech that is applicable across various regulated industries. By leveraging technologies such as big data analytics, AI, machine learning (ML), RPA, and cloud computing, the proposed architecture aims to automate and enhance regulatory compliance processes.

The authors demonstrate the potential of adoption and integration of RPA with other technologies to boost efficiency as automated processes are faster, safeguarding that compliance tasks are completed within regulatory deadlines [12].

Numerous studies have explored the application of RPA in various business contexts, including compliance screening. For instance, Rohit et al. [13] reviewed data mining techniques for combating money laundering and terrorist financing, providing insights into the potential integration of RPA with data mining tools to optimize compliance processes. They also investigated using data mining approaches for AML and discussed the challenges and benefits of automated solutions in compliance screening [14].

2.5. Gaps in Existing Research

While existing research highlights the potential of RPA in compliance screening, several gaps still need to be addressed. For example, most studies focus on the technical aspects of RPA implementation, with limited attention given to the practical challenges businesses may face when adopting RPA solutions. Additionally, there is a need for more empirical studies that evaluate the effectiveness of RPA in real-world compliance settings, covering both technical and organizational aspects of RPA in compliance [15].

The study conducted by Enriquez et al. [8] highlights that very few papers discuss the specific functionalities of RPA platforms. This lack of discussion may be due to industrial protection or patents, as there is no information on related patents in the field of RPA [8].

In their paper "Anti-Money Laundering by International Institutions: A Preliminary Assessment," Marco Arnone and Pier Carlo Padoan evaluate the effectiveness of the AML/CFT program introduced by the International Monetary Fund (IMF) and the World Bank (WB), in collaboration with the Financial Action Task Force (FATF). The study highlights significant disparities in the implementation of preventive and repressive measures across a 20-country sample, noting that Eurozone countries tend to outperform other regions. Despite substantial progress in repressive measures, the authors identify critical gaps in preventive measures and call for more transparency, consistent quality in assessments, and more frequent follow-up evaluations to ensure continuous improvement in AML compliance[16].

The gaps in the existing research include the integration of AI with RPA, comprehensive support in the analysis phase, robust software testing, understanding the broader impact on organizational performance, and addressing ethical and legal implications [17]. However, this thesis focuses on the application of RPA in the compliance screening process.

2.6. Conclusion

The literature review reinforces the significance of compliance screening in mitigating risks associated with financial and business crimes and crimes related to terrorism financing. It highlights the challenges businesses face in traditional compliance processes and the potential of RPA to address these challenges, considering all legal and ethical concerns.

While existing research provides valuable insights into the application of RPA in compliance screening, further studies are needed to explore the practical implications and real-world effectiveness of RPA solutions. This thesis aims to contribute to this body of knowledge by developing a Proof of Concept (POC) to demonstrate the applicability and efficiency of RPA in compliance screening.

CHAPTER 3

Research Methodology

Design Science Research (DSR) is the selected methodology for this thesis, with the necessary adaptation. DSR is well-suited for projects that develop and test artifacts to create innovative solutions to practical problems. DSR is distinct from traditional research methodologies due to its focus on generating prescriptive knowledge, or "knowledge-to-improve," which aims to achieve practical outcomes through design and testing [18]. This methodology is iterative and involves refining an artifact to address a specific problem, with each iteration contributing to both the artifact's utility and the theoretical understanding of the problem it addresses [19].

Figure 1, adapted from Bocke et al. [6], shows the iteration phasis of DSR.

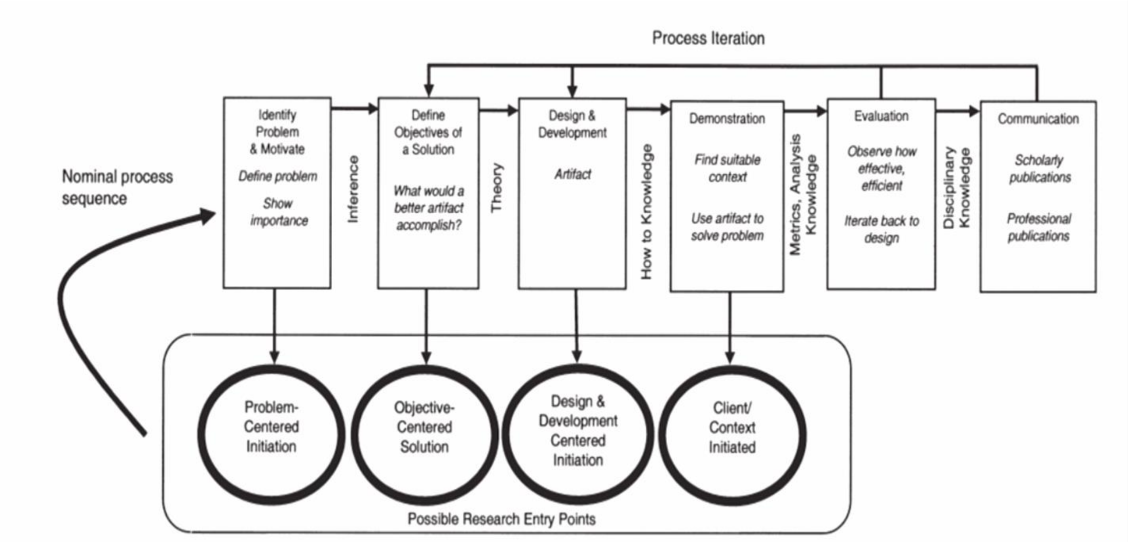


Figure 1- DSR Process. Adapted from Bocke et al.

In its structured form, DSR follows a sequence of six activities outlined by Peffers et al., which guide the process from problem identification to artifact demonstration, evaluation, and communication [20]. These stages allow researchers to iteratively develop and assess solutions while gathering empirical data to support the artifact's relevance and efficacy. This cycle of design, evaluation, and refinement is central to the DSR methodology, as demonstrated in studies that have applied DSR to build systems like web-based dashboards and educational tools [21]. For instance, in their development of a prototype dashboard for construction managers, Gledson et al.[21] used DSR to ensure the artifact met real-world needs by iterating based on feedback and refining the solution to improve productivity and coordination.

The DSR framework summarized in Figure 2, adapted from Bocke et al. [6], shows how different phases of the process interact with each other and how it's possible to redesign and rebuild form knowledge.

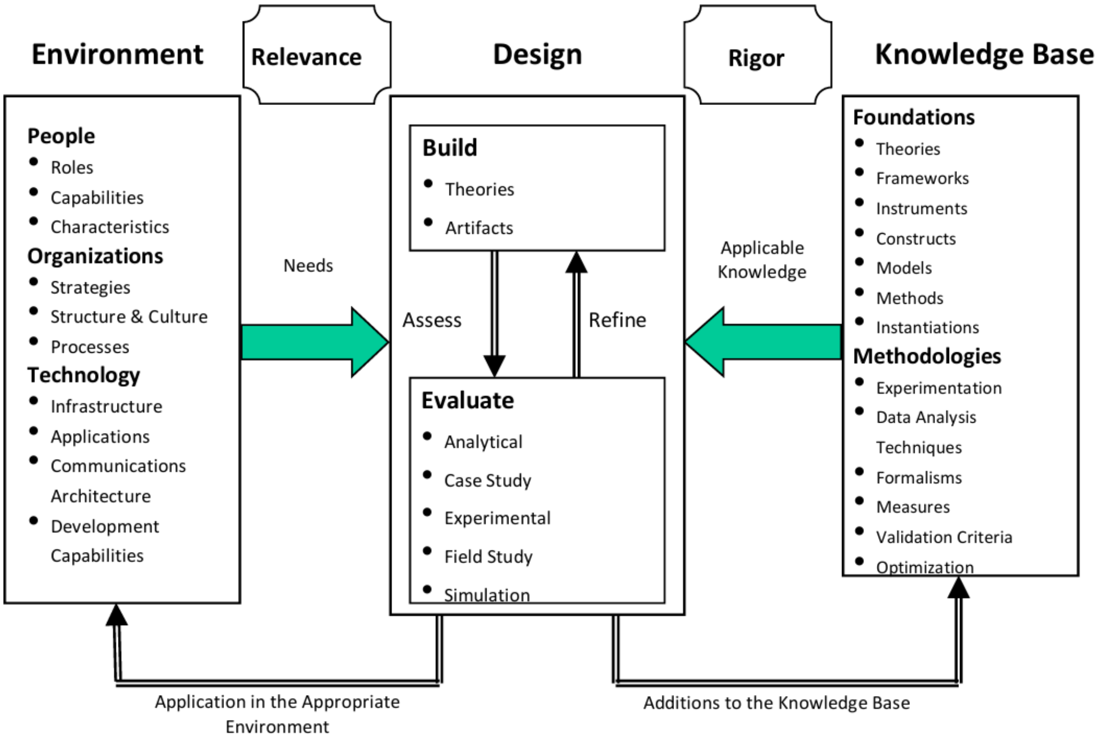


Figure 2- DSR Framework. Adapted from Brocke et all.

DSR's flexibility across fields has been widely recognized, allowing its use in domains ranging from information systems and engineering to applied psychology [18]. Its value lies in bridging theoretical insights with actionable practices, often through industry-academic partnerships that ensure the solutions are directly applicable to practitioner needs. By adopting DSR, this thesis project aligns with a structured yet adaptable framework that supports both the theoretical and practical development of the compliance screening tool, ensuring it is rigorously evaluated and aligned with the needs.

CHAPTER 4

Proof of Concept and Evaluation

As highlighted in the previous sections of this thesis, traditional compliance methods reliant on manual processes are often plagued by errors, high costs, and inefficiency. To overcome these challenges, this Proof of Concept (POC) introduces an RPA-driven solution designed to automate the extraction, compilation, and harmonization of sanctions lists. By automating the compliance screening process, this POC aims to reliably identify individuals or entities appearing on sanctions lists, optimize operational expenses and resource allocation, and boost the overall speed and effectiveness of compliance measures.

Figure 3 illustrates the processes followed for the development of the RPA screening tool.

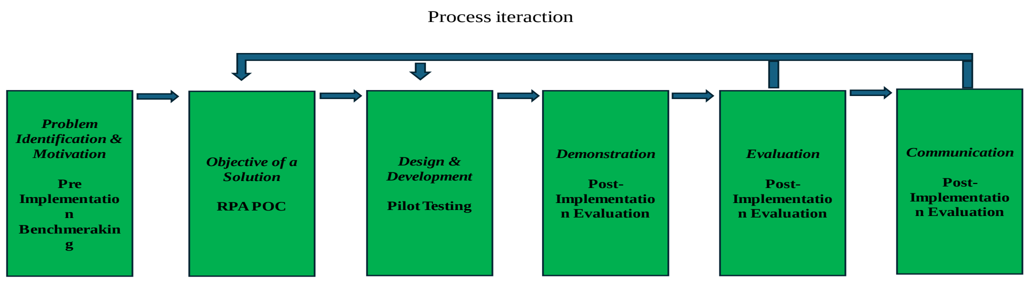


Figure 3- Process Iteration

Pre-Implementation Benchmarking provides the initial information, identifying existing problems with manual processes. This information feeds into the Problem Identification phase of the DSR.

Pilot Testing is where the POC is deployed to demonstrate its potential solution. Metrics and user feedback help in Design & Development and Objective of a Solution by identifying any needed refinements.

Post-Implementation Evaluation compares post-deployment results with the pre-implementation benchmarks. It aligns with the Evaluation and Communication phases of DSR by analyzing performance improvements, documenting user feedback, and providing insights for potential further iterations.

4.1. System Design

The POC's system architecture comprises four core modules designed to automate the sanctions screening process: Data Extraction, Data Compilation, Screening, and Reporting & Audit.

The Data Extraction Module retrieves sanctions data from multiple sources, including the UN and the EU. To guarantee data accuracy and currency, the system is configured to update sanctions lists regularly, ensuring that the latest information is always accessible for screening purposes.

The Data Compilation Module acts as a central repository for consolidating data from various sources. It standardizes the extracted information into a unified format, resolving discrepancies and inconsistencies to create a coherent and usable dataset. This harmonization allows for effective screening and analysis.

The Screening Module leverages RPA to conduct real-time comparisons between transaction and business data and the compiled sanctions lists. By automating this process, the system can promptly identify potential matches, flagging suspicious information for further investigation by human analysts.

The Reporting and Audit Module generates reports detailing the screening activities, providing insights into the system's performance and effectiveness. Additionally, this module maintains a detailed audit trail, documenting all system actions and decisions, for regulatory compliance and internal control purposes.

Figure 4 presents a visual summary of the system's modules and how they interact.

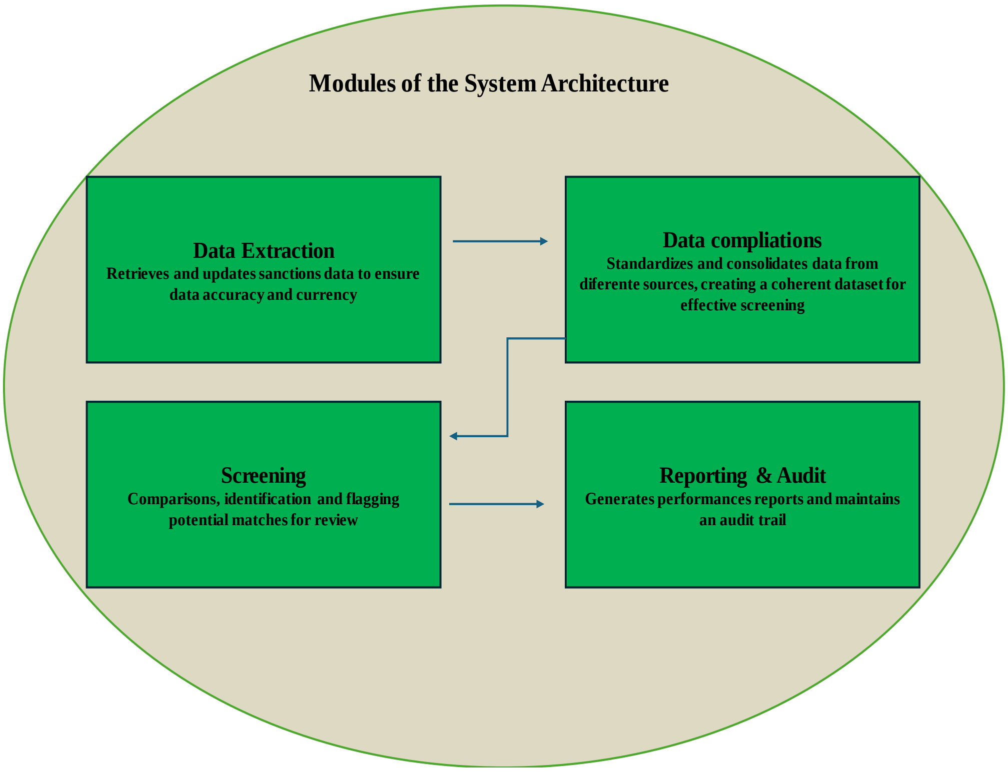


Figure 4- Modules of the RPA System

4.2. System Workflow

The system workflow outlines the sequential steps involved in the sanctions screening process, from data acquisition to reporting.

Data Extraction

The workflow commences with the Data Extraction phase. The RPA bot is deployed to access and retrieve relevant information from designated online sanctions list repositories. The extracted data is subsequently stored in a centralized database for processing.

Data Harmonization

Once the data is collected, the Data Harmonization process begins. This stage involves standardizing and formatting the extracted data to ensure consistency across different data sources. Any duplicate records or discrepancies are identified and rectified to maintain data integrity.

Compliance Screening

The core of the system is the Compliance Screening phase. Business data is fed into the system for analysis and the RPA bot then cross-reference this data against the harmonized sanctions list. Any potential matches or anomalies that indicate potential sanctions violations are flagged for further investigation.

Reporting and Auditing

To increase transparency and accountability, the system generates reports on the screening process, including the number of items screened, the number of potential matches identified. Additionally, a detailed audit trail is maintained, recording all actions performed by the RPA.

Figure 5 demonstrates the system's workflow, which was created by leveraging the Unified Modelling Language (UML) activities diagram.

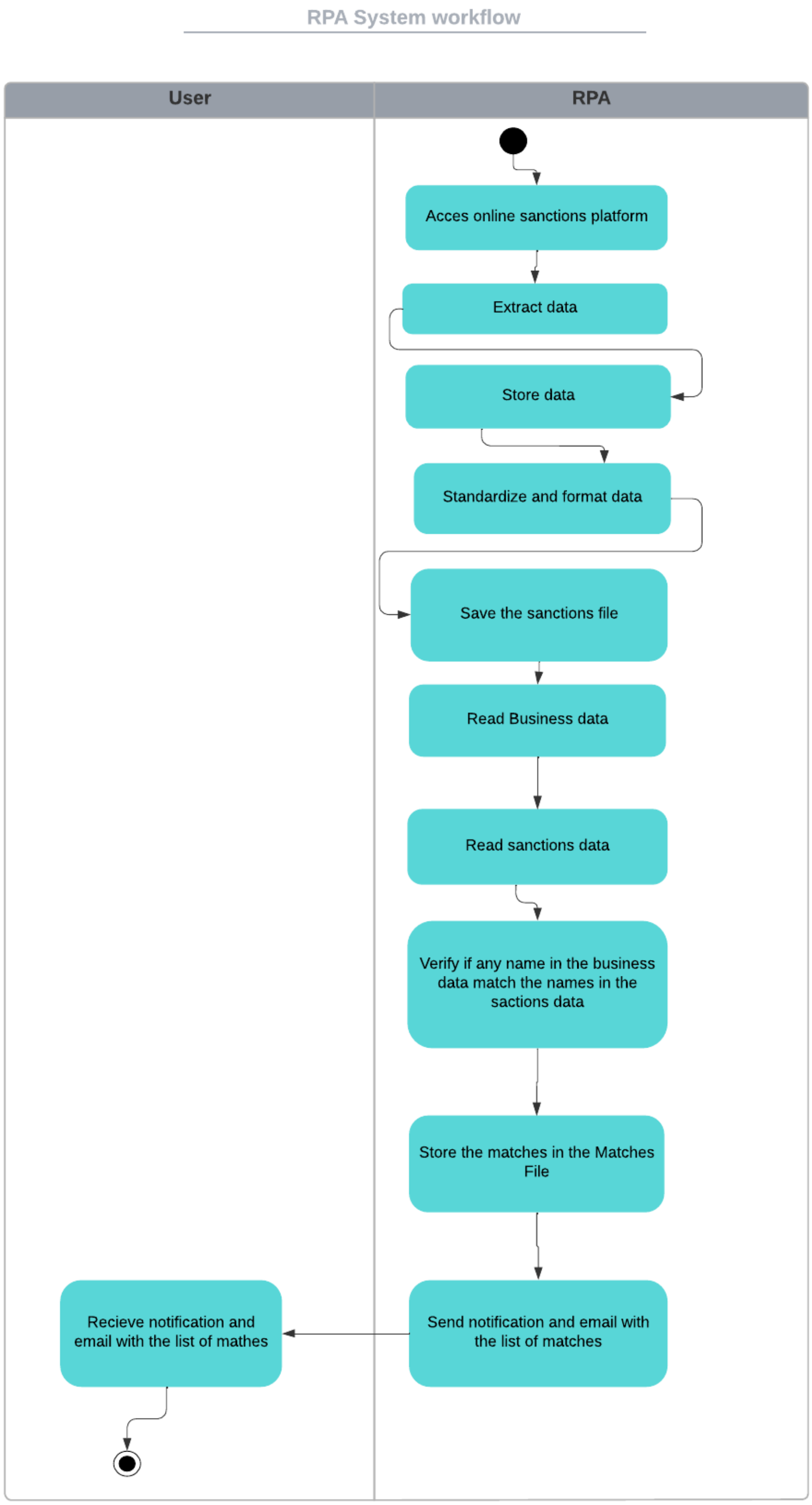


Figure 5- The RPA System Workflow Diagram

4.3. Expected Outcomes

The implementation of this RPA-based compliance screening system is anticipated to deliver several key benefits.

By automating routine and time-consuming compliance tasks, the system will reduce the time and resources required for the overall screening process. Additionally, the system's ability to rapidly process large volumes of transaction data will expedite the identification of suspicious activities, enabling faster response times.

A primary advantage of this system is the elimination of human error, which is a common source of compliance failures. By relying on automated processes and data validation, the system will ensure consistent and reliable screening outcomes, thereby reducing the risk of false positives or negatives.

4.4. Prototype Development

In the prototype for automating compliance screening, a critical step was to select an appropriate RPA platform that could effectively meet the project's requirements and interact successfully with data sources and the extracted data. The decision-making process involved exploring various RPA solutions available in the market, including Power Automate, UiPath, and other leading platforms. The initial phase focused on understanding the capabilities and limitations of different RPA systems.

RPA Technology

Initially, Power Automate emerged as a strong candidate due to its ease of integration with Microsoft products and its user-friendly interface. Power Automate’s drag-and-drop functionality made it a viable option for quickly setting up automation workflows.

Despite Power Automate's advantages, several challenges were encountered during the development process. These challenges prompted a reevaluation of the initial choice, leading to the consideration of UiPath as a more suitable platform for the prototype.

One of the key challenges encountered with Power Automate was its limited capability in handling complex Excel file operations, particularly when working with large datasets and performing multi-file comparisons. While Power Automate offers user-friendly integration with Microsoft Excel, it struggled with tasks that required advanced data manipulation and cross-referencing between multiple files.

For example, extracting data to Excel files and applying Text to Column function for standardization and formatting proved difficult. Power Automate had limitations in iterating through multiple Excel files efficiently. This made it challenging to automate the comparison of business data against the compiled sanctions lists, which is a critical requirement for the compliance screening process. These challenges prompted a transition to UiPath, which provided more robust features for Excel file handling and advanced data manipulation.

UiPath was selected as the final choice for the prototype development. The decision was driven by UiPath’s capabilities in handling complex workflows, its extensive integration options, and its ability to scale effectively. While Power Automate proved useful for preliminary exploration and simpler tasks, UiPath’s features, and robustness provided the necessary foundation to develop a reliable compliance screening solution prototype.

During the system development phase, UiPath proved to be particularly effective in handling and processing data in Excel, especially after the initial extraction and download of sanctions list data. One key advantage of UiPath was its capability to interact with Excel files, providing robust tools for data manipulation.

A specific example of UiPath's efficiency is its ability to apply the Text to Columns function automatically. This feature was instrumental in splitting concatenated data fields, such as full names and additional identifiers, into separate columns for better clarity and organization. By automating this task, UiPath ensured that the data was properly structured before the comparison phase, eliminating the need for possible manual intervention and minimizing the risk of formatting inconsistencies. These capabilities contributed significantly to the overall accuracy and speed of the compliance screening process, highlighting UiPath's suitability for complex, data-intensive tasks in this POC.

In Figures 3 and 4 below, the UiPath Studio is visible, and a sneak preview of the flows related to the screening process, from data extraction to reporting, is provided.

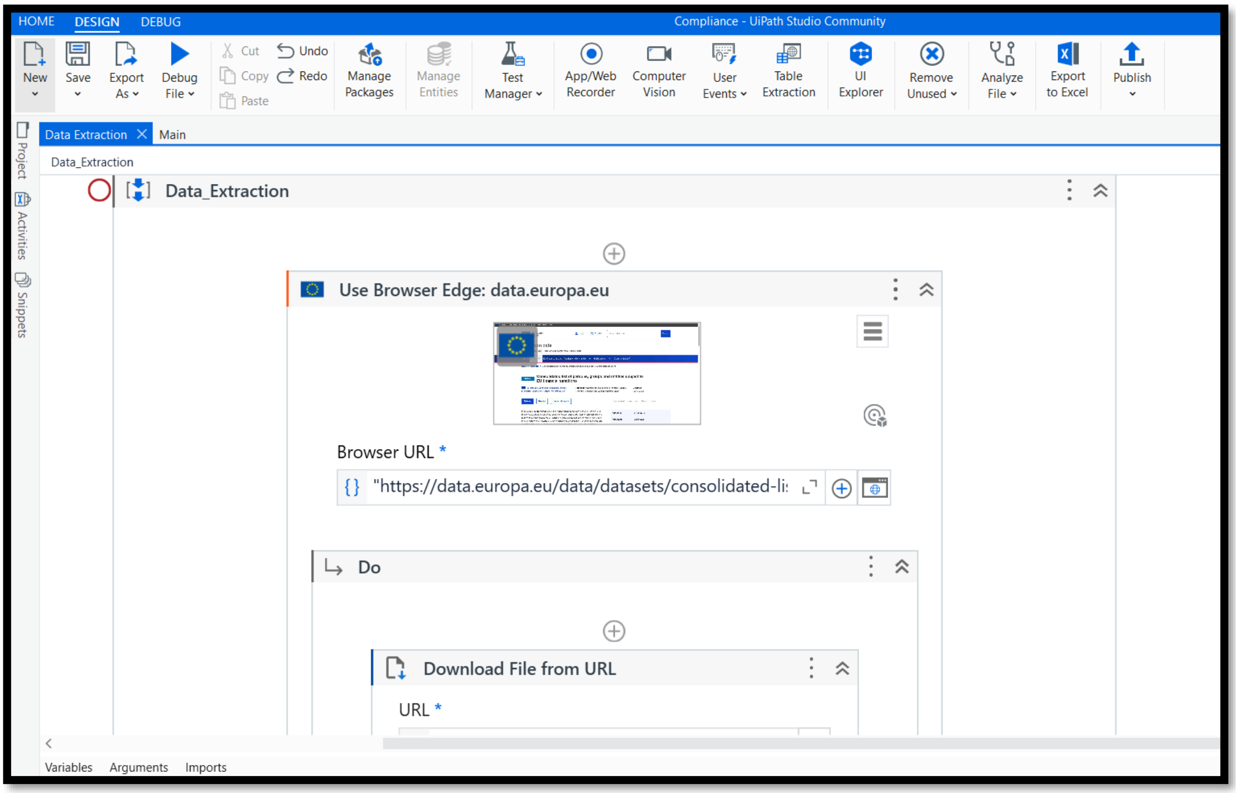


Figure 6-UiPath Studio- Data Extraction and Compilation Flow

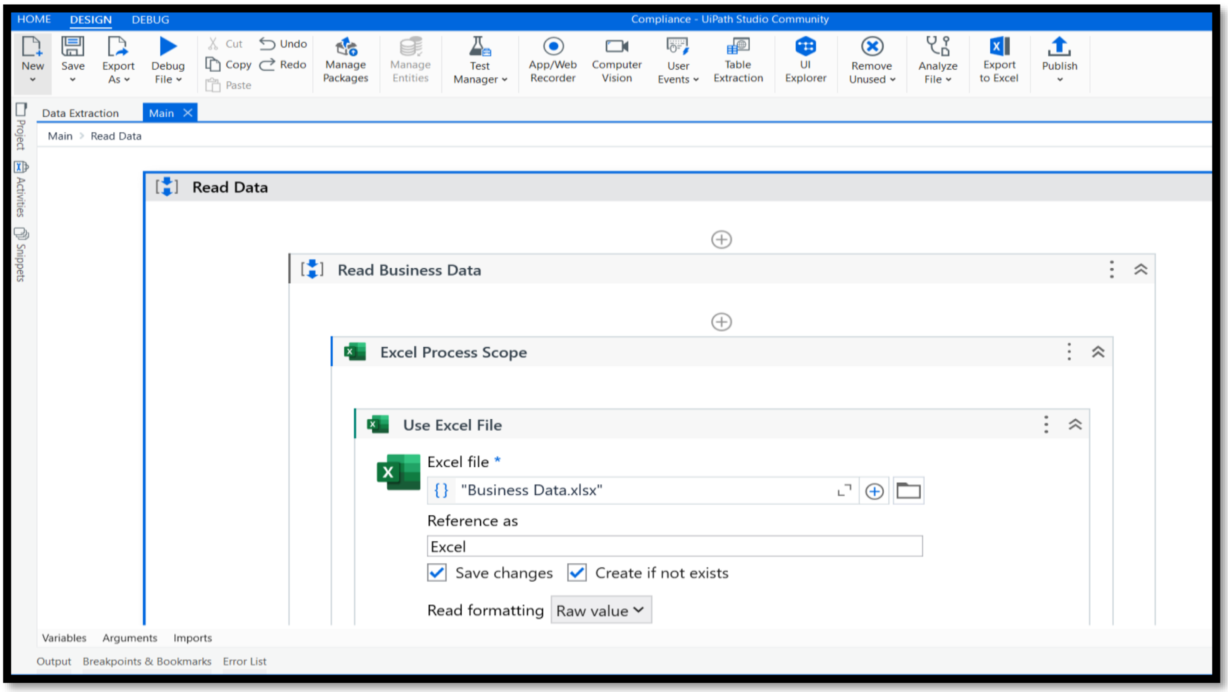


Figure 7- UiPath Studio- Screening and Reporting Flow

Sanctions Data Source

The data utilized for the development was sourced from sanctions lists compiled by the EU, due to their comprehensive coverage and regular updates, which are essential for accurate and effective compliance screening. Additionally, these lists include sanctions imposed by the UN, making them a consolidated and reliable source of information for identifying individuals, entities, and organizations subject to international sanctions.

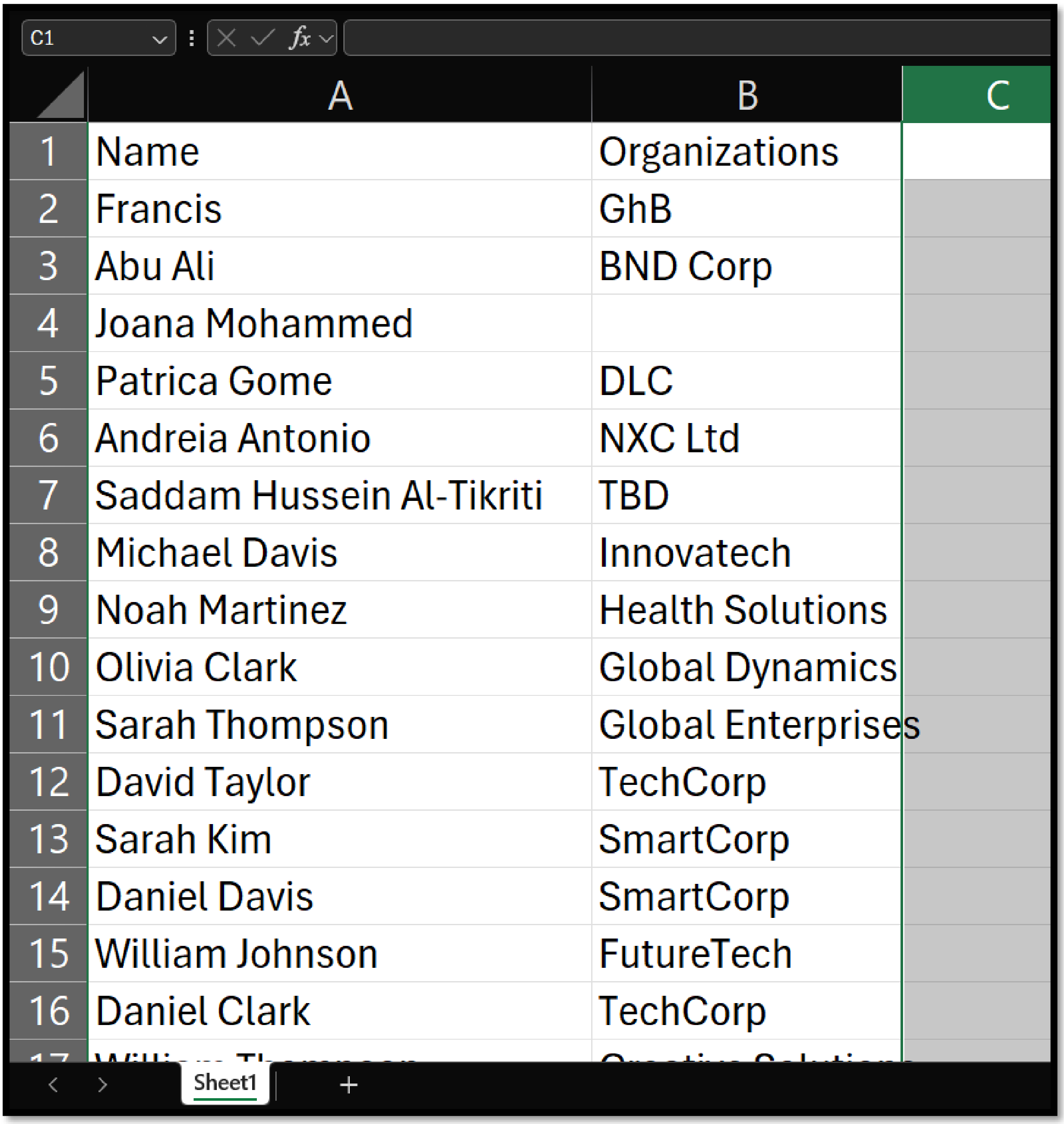
The names in the business data are read and compared with the sanctions list data to identify matches. Figures 7 and 8 sample these tables below.

R1 | Naal_wholename

	A	B	C	D	E	F	G	H	I	P	Q	R	S
1	Date_file	Entity_logi	Subject_ty	Leba_num	Leba_publica	Leba_url	Programm	Entity_ren	Naal_logic	Naal_firstr	Naal_midd	Naal_wholenam	Naal_gend
2	29/10/202	13	P	1210/200:	08/07/2003	http://eur	IRQ	(UNSC RES	17	Saddam		Saddam Hussein	M
3	29/10/202	13	P	1210/200:	08/07/2003	http://eur	IRQ	(UNSC RES	19			Abu Ali	
4	29/10/202	13	P	1210/200:	08/07/2003	http://eur	IRQ	(UNSC RES	380			Abou Ali	
5	29/10/202	13	P	1210/200:	08/07/2003	http://eur	IRQ	(UNSC RESOLUTION 1483)					
6	29/10/202	13	P	1210/200:	08/07/2003	http://eur	IRQ	(UNSC RESOLUTION 1483)					
7	29/10/202	20	P	1210/200:	08/07/2003	http://eur	IRQ	(Saddam's	26	Qusay	Saddam	Qusay Saddam H	M
8	29/10/202	20	P	1210/200:	08/07/2003	http://eur	IRQ	(Saddam's	381	Qoussaï	Saddam	Qoussaï Saddam	Hussein Al
9	29/10/202	20	P	1210/200:	08/07/2003	http://eur	IRQ	(Saddam's second son)					
10	29/10/202	20	P	1210/200:	08/07/2003	http://eur	IRQ	(Saddam's second son)					
11	29/10/202	20	P	1210/200:	08/07/2003	http://eur	IRQ	(Saddam's second son)					
12	29/10/202	23	P	1210/200:	08/07/2003	http://eur	IRQ	(Saddam's	29	Uday	Saddam	Uday Saddam Hu	M
13	29/10/202	23	P	1210/200:	08/07/2003	http://eur	IRQ	(Saddam's	383	Oudaï	Saddam	Oudaï Saddam Hussein Al-T	
14	29/10/202	23	P	1210/200:	08/07/2003	http://eur	IRQ	(Saddam's eldest son)					
15	29/10/202	23	P	1210/200:	08/07/2003	http://eur	IRQ	(Saddam's eldest son)					
16	29/10/202	23	P	1210/200:	08/07/2003	http://eur	IRQ	(Saddam's eldest son)					
17	29/10/202	25	P	1210/200:	08/07/2003	http://eur	IRQ		31			Abid Hamid Mah	M
18	29/10/202	25	P	1210/200:	08/07/2003	http://eur	IRQ		32			Abid Hamid Bid H	M
19	29/10/202	25	P	1210/200:	08/07/2003	http://eur	IRQ		34			Abdel Hamid Ma	M
20	29/10/202	25	P	1210/200:	08/07/2003	http://eur	IRQ		35			Abed Mahmoud	M
21	29/10/202	25	P	1210/200:	08/07/2003	http://eur	IRQ		384			Abid Hamid Mahmoud Al-Ti	
22	29/10/202	25	P	1210/200:	08/07/2003	http://eur	IRQ		385			Abid Hamid Bid Hamid Mah	

Sanctions_List

Figure 8-Sanctions Data



	A	B
1	Name	Organizations
2	Francis	GhB
3	Abu Ali	BND Corp
4	Joana Mohammed	
5	Patrica Gome	DLC
6	Andreia Antonio	NXC Ltd
7	Saddam Hussein Al-Tikriti	TBD
8	Michael Davis	Innovatech
9	Noah Martinez	Health Solutions
10	Olivia Clark	Global Dynamics
11	Sarah Thompson	Global Enterprises
12	David Taylor	TechCorp
13	Sarah Kim	SmartCorp
14	Daniel Davis	SmartCorp
15	William Johnson	FutureTech
16	Daniel Clark	TechCorp

Figure 9-Business Data

Result of the screening process

After the screening process is completed, the system notifies the user of the completion of the process execution, as shown in Figure 10, and then sends an email to the user with the possible matches, example shown in Figure 11.

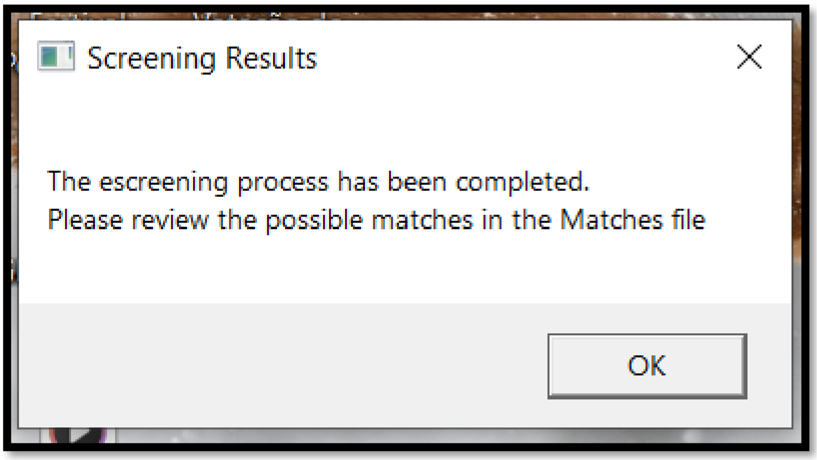
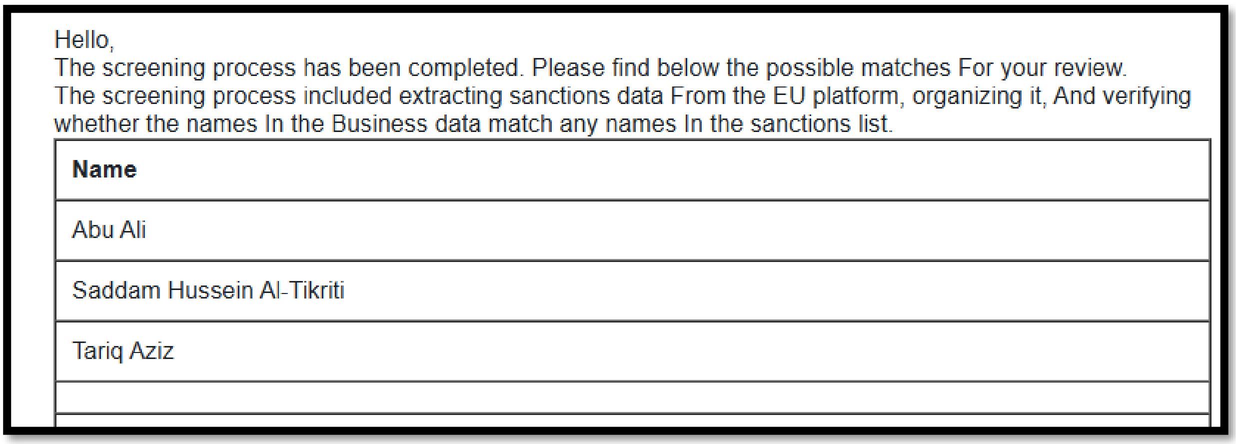


Figure 10- Notification- Screening Results


Hello,
The screening process has been completed. Please find below the possible matches For your review.
The screening process included extracting sanctions data From the EU platform, organizing it, And verifying whether the names In the Business data match any names In the sanctions list.

Name
Abu Ali
Saddam Hussein Al-Tikriti
Tariq Aziz

Figure 11- email to user with the screening results

The match cases from the screening process are also stored in an Excel file that is available for the user, as demonstrated in Figure 11 below.

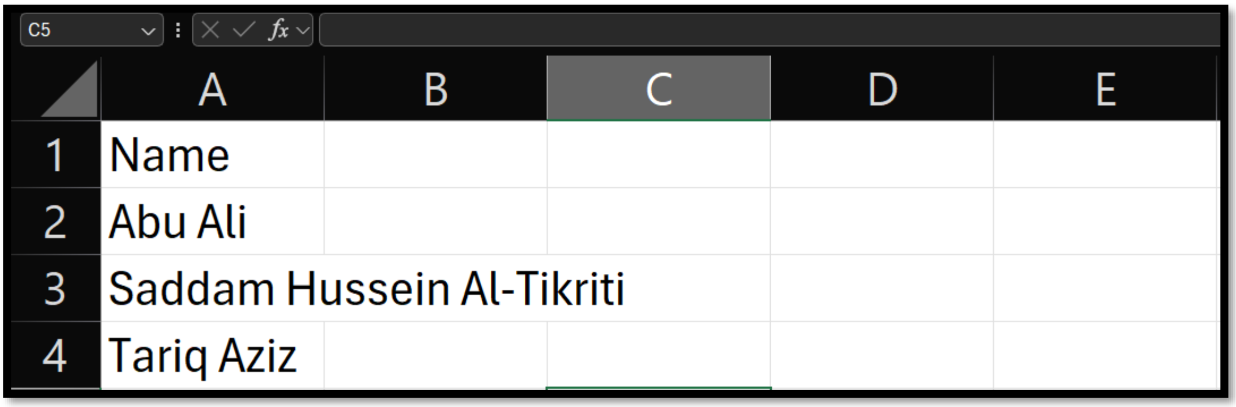

	A	B	C	D	E
1	Name				
2	Abu Ali				
3	Saddam Hussein Al-Tikriti				
4	Tariq Aziz				

Figure 12- Matches

4.5. Evaluation Planning

The success of the RPA System for automating compliance screening hinges on a structured evaluation plan. This plan outlines the approach and criteria to assess the effectiveness, efficiency, and overall value of the RPA-driven system in achieving its intended objectives. The evaluation will focus on key performance indicators (KPIs) that align with the expected outcomes and goals detailed in previous sections of this thesis.

The primary goal of the evaluation is to assess the overall performance and impact of the RPA-based sanctions screening system. To achieve this, the evaluation focuses on the measurements described in Table 2, developed following the Framework created by Kim S.-H [22] that offers guidelines on the selection and evaluation of RPA solutions.

Table 2- Evaluation Planning. Adapted from Kim S.-H Framework

Measurement	Description
Accuracy Assessment	Determine the system's precision in identifying individuals and entities listed on sanctions lists. This includes evaluating the system's ability to correctly match names.
Efficiency Measurement	Quantify the time saved and resource optimization achieved through the automation of the compliance screening process. This will involve comparing the performance of the RPA-based system to manual screening.
User Experience Evaluation	Gather feedback from end-users to assess the system's usability, user interface, and overall satisfaction. This input will be used to identify areas for improvement and enhance the user experience

4.6. Evaluation Criteria and Key Performance Indicators (KPIs)

Combining Kim's S.-H.[22] framework with Patricio et al.[23] 's paper on sustainable implementation of RPA, a set of evaluation criteria, and corresponding KPIs are employed to comprehensively assess the system's performance, as summarized in Table 3.

Table 3- Evaluation Criteria and KPI's

Evaluation Category	Objective	Metrics	Evaluation Method
Accuracy	Evaluate the system's precision in identifying matches between transaction data and sanctions lists.	- True Positive Rate: Percentage of correctly identified entities that are on sanctions lists.	The system will be tested using a dataset with known entities on sanctions lists. Results will be compared to manual screening processes for accuracy assessment.
		- False Positive Rate: Percentage of entities incorrectly flagged as matches.	
		- False Negative Rate: Percentage of missed entities that are on sanctions lists.	
Efficiency	Measure the speed and resource efficiency of the automated compliance screening process.	- Average Processing Time: Time taken to screen each transaction.	Monitor and record processing times during pilot runs. Analyze throughput data to quantify speed and efficiency improvements.
		- Total Throughput: Number of items processed in a specific timeframe.	
		- Reduction in Manual Effort: Comparison of resources used in manual versus automated processes.	
User Feedback	Ensure the system meets the expectations	- User Satisfaction: feedback on usability, interface, and performance.	Collect feedback from users

4.7. Iterations and Evaluation Processes

The evaluation process will be conducted in two main phases to assess the performance and impact of the RPA-based sanctions screening system.

Pre-Implementation Benchmarking

The pre-implementation benchmarking phase involved gathering insights from the literature and analyzing available sanctions lists, particularly those compiled by the European Union and the United Nations. This process provided a clear understanding of traditional compliance practices, their limitations, and emerging trends in the sector. The analysis also highlighted a growing need for scalable compliance solutions due to increasing regulatory complexity.

Pilot Testing

The POC has been tested in a controlled environment using data to simulate production conditions. Performance metrics will be closely monitored across all defined KPIs to assess the system's capabilities and identify any technical issues or areas requiring refinement.

Post-Implementation Evaluation

Once the system has been operational for a specified period, a comprehensive evaluation will be conducted. The performance data collected during the pilot phase will be compared to the pre-implementation benchmarks to measure overall improvement. User feedback will be solicited to gauge user satisfaction, identify areas for improvement, and ensure the system aligns with end-user needs.

4.8. Reporting and Analysis

Upon completion of the evaluation process, a report will be generated, consolidating the findings and insights gathered. This report will detail the system’s performance against the established KPIs, highlighting areas of strength and areas requiring improvement.

Key findings and recommendations will be presented to relevant stakeholders, including executive management, compliance teams, and IT departments. This presentation will emphasize the system's successes in enhancing efficiency, accuracy, and cost-effectiveness. Additionally, opportunities for further development and optimization will be discussed.

Based on the evaluation results and stakeholder feedback, recommendations for next steps will be formulated. These may include suggestions for system upgrades, expansion to additional business units, or integration with other compliance systems. The goal is to provide a clear roadmap for maximizing the system's value and impact within the organization.

4.9. Evaluation Results

The RPA-based compliance screening system was evaluated across key performance metrics: accuracy, efficiency, and user feedback. The results of these evaluations revealed the system's effectiveness in automating and optimizing compliance processes, as illustrated in Table 4.

Table 4- Evaluation Results

Criteria	Indicator	Value	Notes
Accuracy	True Positive Rate: The percentage of correctly identified entities that are on sanctions lists.	100%	Identified 13 out of 13 names present both in the business data and the sanctions list
	False Positive Rate: The percentage of entities incorrectly flagged as matches.	0%	No name was incorrectly identified as a match
	False Negative Rate: The percentage of missed entities that are on sanctions lists	0%	None of the names present both in the business data and the sanction list were missed.

Efficiency	Average Processing Time: The time taken to screen each individual transaction through the system	2,8 seconds	Processing time per item = Total processing time / Number of items = 6 minutes / 127 items ≈ 0.0472 minutes/item; Processing time per item ≈ 0.0472 minutes/item * 60 seconds/minute ≈ 2.83 seconds/item
	Total Throughput: The number of items processed within a specific timeframe	727 items in 6 Minutes	127 items on the business data plus 600 items from the sanctions data
	Reduction in Manual Effort: Comparison of time spent on manual screening versus the automated process	94%	Duration of manual effort to screen 127 items from the business: 93 Minutes; Durations of the automated process: 6 minutes; 93-6=87; (87/93) *100
User Feedback	feedback on usability, interface, and performance	The tool meets the expectations and provides a more efficient screening process	

The system achieved a high True Positive Rate, correctly identifying 100% of entities on the sanctions lists that were present in the business data, with no false positives or false negatives observed. This result underscores the system's capability to match transaction data against sanctions lists with precision, ensuring comprehensive compliance coverage.

The system achieved a zero false positive rate and zero false negative rate, demonstrating exceptional accuracy. This outcome can be attributed to the design of the matching algorithm, which focuses on exact matches between names in the business data and those listed on the sanctions lists. The system employs a deterministic approach, where it searches for precise, character-by-character matches without attempting to interpret variations, such as differences in spelling or formatting.

The average processing time for screening each transaction was recorded at approximately 2.8 seconds, demonstrating significant time savings compared to manual methods. The system processed 727 items in 6 minutes, comprising 127 items from the business data and 600 from sanctions lists. This rapid processing represents a 94% reduction in manual effort when compared to manual screening conducted in the evaluation of the POC.

Usability feedback indicated that the tool met the expectations and offered a streamlined, more efficient screening process.

CHAPTER 5

Conclusion

This thesis demonstrated the development and evaluation of an RPA-based system designed to enhance compliance screening by automating the extraction, compilation, and comparison of sanctions lists with business data. The POC addressed key compliance challenges such as inefficiency, high operational costs, and the risk of human error inherent in manual processes. The use of the DSR methodology allowed for an efficient process of artifact development, evaluation, and refinement, resulting in a solution that aligns with the identified needs.

The evaluation results confirmed that the RPA solution significantly improved the speed and accuracy of compliance screening. The system's ability to process data rapidly, reduce human involvement, and maintain accuracy supports its potential as a valuable tool for financial institutions and other organizations facing complex compliance requirements.

This research shows that RPA can significantly transform compliance operations by optimizing processes and enhancing overall efficiency. The findings demonstrates that financial institutions and other organizations can achieve lower operational costs and faster responses to compliance requirements through the strategic implementation of RPA. The project's success highlights how RPA-based systems offer a tangible solution to the challenges posed by traditional, labor-intensive compliance methods.

From an academic standpoint, this study contributes valuable insights into the application of the DSR methodology in developing innovative compliance solutions, which was critical in refining the artifact, as it allowed for continuous testing and improvement. This ensured that the final system was not only functional but also aligned with the needs and the set goals.

Key findings from the evaluation phase underscore the effectiveness of RPA in handling high-volume, repetitive tasks with greater speed and accuracy than manual methods. Specifically, the system achieved a 94% reduction in manual screening time, demonstrating its potential to optimize compliance practices. This result solidifies the position of RPA as an essential tool for enhancing operational efficiency in compliance processes.

Moreover, the research supports the broader movement toward digital transformation in regulatory practices, showing that technologies like RPA can automate and optimize compliance tasks to create more agile and responsive systems. This aligns with the current push in industries to embrace digital solutions that promote flexibility and adaptability in the face of evolving regulatory landscapes.

While the POC focused on sanctions list screening, the underlying principles and design can be scaled and adapted to other compliance areas. This approach's sustainability suggests that similar models could be employed across industries to support long-term, automated compliance solutions. This framework's flexibility means that organizations can implement RPA in various compliance processes and other business areas, thus supporting sustainable and efficient operations.

Finally, this project demonstrates that integrating automation into existing technological ecosystems is both feasible and beneficial. It paves the way for future advancements that could involve the integration of RPA with AI, machine learning, and other sophisticated technologies, leading to even more powerful and proactive compliance tools. This research thus serves as a foundation for future exploration and development, contributing to a vision of more automated, accurate, and efficient compliance management systems.

5.1. Limitations

Despite the positive outcomes, this research had limitations that need to be addressed. The evaluation was conducted within a controlled environment, which may not entirely replicate the variability found in live operational settings. Additionally, while the system demonstrated effective handling of structured data, it may require further development to process unstructured data sources or adapt to changes in sanctions list formats. Finally, the evaluation focused on technical performance but did not extensively cover potential integration challenges or long-term scalability beyond the scope of the prototype development and testing.

While the approach focuses on exact matches between names in the business data and those listed on the sanctions lists ensure high accuracy by eliminating the risk of false positives (incorrectly flagged entities) and false negatives (missed entities), it relies on the assumption that the data is consistently formatted across all sources. The exact match strategy works well in controlled environments where data quality is high, and variations are minimal. However, it may be less effective in scenarios where names are represented differently due to typographical errors, alternative spellings, or cultural naming conventions. This limitation highlights a potential area for future improvement, where another technology could be introduced to handle such variations while maintaining low error rates.

Integration with existing IT infrastructure also presents a potential challenge. The RPA solution needs to interact seamlessly with various legacy systems, databases, and third-party applications used by institutions. Differences in system architectures and data formats could complicate this integration process, leading to additional development and customization efforts. Furthermore, the sensitive nature of compliance data raises concerns about data privacy and security. Ensuring that the RPA system complies with data protection regulations (e.g., GDPR) and incorporates robust security measures is critical to avoid potential legal and ethical issues.

Another limitation of the prototype is that there was no iteration beyond the initial testing phase, which was expected to happen after collecting substantial feedback from compliance officers. Finally, the post-implementation evaluation was not conducted due to the focus on testing and evaluating the prototype in a controlled environment.

5.2. Future Work

Future research should explore expanding the system's capabilities to include the integration of AI and machine learning for advanced data analysis and anomaly detection. This would enable the system to handle more complex compliance scenarios and adapt to evolving regulatory requirements. Additionally, deploying the system in a live production environment and conducting longitudinal studies could provide more comprehensive insights into its long-term performance and scalability. Further studies could also assess the system's adaptability to other compliance-related tasks, such as Know Your Customer (KYC) processes and fraud detection, broadening its applicability in multiple business sectors.

While the prototype was rigorously tested in a controlled environment, future work should focus on deploying the system in a live production setting to better understand its performance. Testing in a controlled environment was necessary to ensure initial functionality, validate the system's design, and minimize external variables that could affect the evaluation. However, live environments present additional complexities such as network latency, variable data quality, and diverse data formats that were not fully replicated during the prototype phase.

To gain a comprehensive assessment of the system's robustness and scalability, future research should involve continuous evaluation conducted in operational settings. This would allow for monitoring the system's long-term performance, adaptability to changing sanctions lists, and integration with existing IT infrastructure. Additionally, testing with real transaction data in a live environment could provide deeper insights into how the system handles data inconsistencies, fluctuating volumes, and potential integration challenges, ultimately contributing to its refinement and broader applicability.

Extending the RPA system's capability to handle unstructured data, such as emails, scanned documents, and diverse text formats, could be explored by future research. This would make the system more adaptable to different types of data inputs and further automate the screening process by incorporating natural language processing (NLP) to extract and interpret relevant information. Additionally, explore the potential for integrating the RPA solution with other compliance tools, such as Customer Relationship Management (CRM) systems and enterprise resource planning (ERP) platforms. This would create a unified compliance ecosystem, improving data flow and collaboration across departments.

Bibliography

[1] L. D. Pellegrina e D. Masciandaro, «The Risk-Based Approach in the New European Anti-Money Laundering Legislation: A Law and Economics View», *"Paolo Baffi" Cent. Cent. Bank. Financ. Regul.*, 2008.

[2] R. Caruso, «The Impact of International Economic Sanctions on Trade An empirical Analysis», *Univ. Cattolica Sacro Cuore Milano*, 2003.

[3] D. Harry, S. H. Nicole, J. Albert, e J. Ritcey-Donohue, «International Anti-Money Laundering», *Int. Leg. Dev.*, vol. 53, 2019.

[4] A. Ramadhan e N. Afriliana, «The Trends and Roles of Robotic Process Automation Technology in Digital Transformation: A Literature Review», *J. Syst. Manag. Sci.*, doi: 10.33168/JSMS.2022.0303.

[5] B. Firmansyah e A. A. Arman, «Generic Solution Architecture Design of Regulatory Technology (RegTech)», *Indones. J. Electr. Eng. Inform. IJEEI*, vol. 11, n.º 2, 2023.

[6] J. vom Brocke, A. Hevner, e A. Maedche, «Introduction to Design Science Research», *Des. Sci. Res.*, doi: https://doi.org/10.1007/978-3-030-46781-4_1.

[7] P. R EUTER e E. D. T RUMAN M., «Anti-Money Laundering Overkill?», *Int. Econ.*, 2005.

[8] J. G. J. G. ENRÍQUEZ, A. JIMÉNEZ-RAMÍREZ, F. J. DOMÍNGUEZ-MAYO, e J. A. GARCÍA-GARCÍA, «Robotic Process Automation: A Scientific and Industrial Systematic Mapping Study», *IEEE Access*, vol. 8, pp. 39113–39129, 2020.

[9] A. Merz, «'It could have been us'. Peer responses to money-laundering violations in the Dutch banking industry», *Crime Law Soc. Change*, vol. 81, n.º 3, pp. 281–300, 2024, doi: 10.1007/s10611-023-10120-y.

[10] A. E. M. Shokry, M. A. Rizka, e N. M. Labib, «Counter terrorism finance by detecting money laundering hidden networks using unsupervised machine learning algorithm».

[11] I. Zavoli e C. King, «The Challenges of Implementing Anti-Money Laundering Regulation: An Empirical Analysis», *Mod. Law Rev.*, vol. 84, n.º 4, pp. 740–771, 2021, doi: 10.1111/1468-2230.12628.

[12] S. Aguirre e A. Rodriguez, «Automation of a Business Process Using Robotic Process Automation (RPA): A Case Study», *Springer Int. Publ. AG*, pp. 65–71, 2017, 2017.

[13] K. D. Rohit e D. Patel B., «Review On Detection of Suspicious Transaction In Anti-Money Laundering Using Data Mining Framework», *Int. J. Innov. Res. Sci. Technol.*, vol. 1, n.º 8, 2015.

[14] N. A. Le Khac, S. Markos, M. O'Neill, A. . Brabazon, e M.-T. Kechadi, «An investigation into Data Mining approaches for Anti Money Laundering», *Proc. 2020 Int. Conf. Emerg. Technol. Comput. ICETiC Lond. UK 2020*, 2020.

[15] J. Siderska, L. Aunimo, T. Süße, J. von Stamm, D. Kedziora, e S. N. B. M. Aini, «Towards Intelligent Automation (IA): literature review on the evolution of Robotic Process Automation (RPA), its challenges, and future trends», *Eng. Manag. Prod. Serv.*, vol. 15, n.º 4.

[16] C. P. Pier e M. Arnone, «Anti-Money Laundering by International Institutions: A Preliminary Assessment», *CIDEI Work.*, n.º 74, 2007.

[17] Lacity, M., & Willcocks, L, «Robotic Process Automation: The Next Transformation Lever for Shared Services», *J. Inf. Technol. Teach. Cases*, p. 9(2), 93–105, 2018.

[18] M. Weggeman e L. Cauffman, «Using design science research to develop and validate the application of client-oriented psychological approaches illustrated by the design of a solution-focused approach», *Methods Psychol.*, vol. 11, p. 100151, dez. 2024, doi: 10.1016/j.metip.2024.100151.

[19] S. Gregor e O. Zwikael, «Design science research and the co-creation of project management knowledge», *Int. J. Proj. Manag.*, vol. 42, n.º 3, p. 102584, abr. 2024, doi: 10.1016/j.ijproman.2024.102584.

[20] J. Figueiredo e F. J. García-Peñalvo, «Design science research applied to difficulties of teaching and learning initial programming», *Univers. Access Inf. Soc.*, vol. 23, n.º 3, pp. 1151–1161, ago. 2024, doi: 10.1007/s10209-022-00941-4.

[21] B. Gledson, K. Rogage, A. Thompson, e H. Ponton, «Reporting on the Development of a Web-Based Prototype Dashboard for Construction Design Managers, Achieved through Design Science Research Methodology (DSRM)», *Buildings*, vol. 14, n.º 2, 2024, doi: 10.3390/buildings14020335.

[22] S.-H. KIM, «Evaluation Criteria for Robotic Process Automation (RPA) Solution», *Electronics*, 2023, doi: https://doi.org/10.3390/electronics12040986.

[23] L. Patrício, L. Costa, L. Varela, e P. Ávila, «Sustainable Implementation of Robotic Process Automation Based on a Multi-Objective Mathematical Model», *Sustainability*, doi: https://doi.org/10.3390/su152015045.