Implementing Robotic Process Automation for Auditing and Fraud Control

Luke Griffiths[1], and Hendrik Willem Pretorius[1][0000-0003-2051-5290]

[1] University of Pretoria, Pretoria, South Africa
Henk.Pretorius@up.ac.za

Abstract. The cost of fraud continues to be a problem for many organizations in the global economy. This study explores how robotic process automation may offer a way forward for organizations to reduce fraud and advance organizational audit effectiveness for detecting potential fraud areas and cases.

The research was performed by conducting a literature review that considered 22 articles (through a selection process) on the relevant research themes of robotic process automation, fraud and auditing.

The findings suggest that organizations should consider robotic process automation as a means for reducing fraud opportunities in organizations. Robotic process automation may also assist organizations to advance their audit efficiency and effectiveness.

The paper conclude by proposing a theoretical framework for the implementation of robotic process automation in fraud control and auditing. A number of new theoretical questions arose during this analysis. This include, the potential use of robotic process automation by fraudsters in support of organizational fraud and secondly, the new skills required by auditors to be effective in an intelligent workplace.

Keywords: Robotic Process Automation, Fraud, Audit, Systematic Literature Review.

1 Introduction

The challenges posed by fraud are significant. The annual, global losses caused by occupational fraud exceeds seven billion US Dollars [1]. One form of occupational fraud, namely asset misappropriation, caused the collapse of various banks in Iran [3]. In general, occupational fraud is widely recognized as a contributing factor to banking crises across the globe [4]. Except for asset misappropriation, other forms of occupational fraud exist namely corruption and financial statement fraud [2].

The significance of fraud as an organisational problem, necessitates the need for an organizational audit function, involved in fraud detecting and control [5]. Organizations should take the necessary precautions to reduce the risk associated with occupational fraud.

One precaution that organizations may consider is the use of robotic process automation. Robotic process automation refers to software tools which automate the execution of tasks by using the same interface that a human actor would [6]. By reducing

repetitive human interaction with computer systems, robotic process automation aims to improve return on investment through automation and streamlined organizational business processes [6]. This is against the backdrop that the most common methods for concealing occupational fraud include the creation of fake physical documents, the creation of fake transactions and the altering of transactions in an accounting system [1]. Minimising interaction with computer systems could potentially decrease the risk of fraud. Robotic process automation may also be beneficial for the audit function by automating many audit tasks [7].

This convergence of technology and people into the same workspace to solve a global problem aligns with the goal of society 5.0 to integrate Industry 4.0 technology with human ideals [29]. Robotic process automation maintains the industrial focus expected from such technology [29] with the goal of addressing illegal, fraudulent activity [7], contributing to the economic advancement envisioned by society 5.0 [30].

The purpose of this systematic literature review is to explore, how robotic process automation may offer ways for organizations to reduce the risk of fraud and advance their audit effectiveness. The study is a generic study, not bound to a specific industry or geographical location.

2 Research Method

The section will briefly discuss the process that was performed during the systematic literature review to answer the following research question:

How can robotic process automation be used in organizations to reduce potential fraud and advance audit effectiveness?

2.1 Search Terms

The following search terms were used in relevant academic journal databases: “robotic process automation” AND (“fraud” OR “audit”)

2.2 Selection Criteria and Quality Assurance

Table 1 presents the selection criteria (what was included and excluded) for the literature review.

Table 1. Selection criteria for the literature review.

Inclusion criteria	Exclusion criteria
1. Peer-reviewed articles.	1. Non peer-reviewed articles.
2. Articles that focus on robotic process automation, auditing and fraud control.	2. Articles whose focus is not robotic process automation, auditing and fraud control.
3. Articles published in the last 3 years for the most current research.	3. Non English articles whose full-text is not available.

4. Relevant articles in any industry and geographic location. 5. Articles published in the last 3 years for the most current research.	4. Articles older than 3 years, for the most current research.

2.3 Source Selection and Data Extraction

The search terms were applied to the following database sources for the literature review: EBSCOhost, ScienceDirect and ProQuest.

The search results were filtered to only include academic works. The database search returned 135 articles. After duplicate articles were removed, 125 articles remained. Article title and abstracts were then screened for relevance and only 66 articles remained. The remaining full-text articles were assessed for appropriateness (using the inclusion and exclusion criteria) and 44 articles were excluded with reasons. Finally, a total of 22 articles were consulted during this literature review, which was carefully captured in Microsoft Excel.

3 Analysis and Discussion

During the systematic literature review, relevant literature themes emerged. These themes are: the automation of mundane tasks (19 relevant articles), process identification for robotic process automation (8 articles), data standardization (5articles), robotic process automation (RPA) vendors (5 articles), the changing role of the auditor (7 articles) and RPA threats (9 articles). A discussion of these literature themes follow.

3.1 Process Automation

The literature indicates that robotic process automation (RPA) is mostly used to automate and replace mundane audit tasks that allow employees and auditors to shift their focus to other organizational tasks [7-25].

Mundane audit tasks involve tasks such as audit evidence gathering [10,25,26], but RPA also saves employees time through automation that helps them to be highly efficient [26]. The time saved allowed employees to focus less on repetitive tasks and more on skill-intensive, value-adding activities such as the use of professional judgement to make decisions [10].

By automating tedious, manual processes, RPA allows auditors to expand the scope of organizational audits [25]. RPA software flag audit exceptions and errors which require expert intervention or further investigation [8,12,21,23,26]. The ability to quickly gather audit evidence across an entire population allows for continuous, real-time analyses of audit evidence [8,23,27].

The nature of RPA as a software solution which performs highly repetitive, predictable tasks also means that the process can be well documented and lead to increased audibility of automated tasks [21-23]. This means that RPA can be programmed to follow control requirements and therefore increase confidence in control tests [23] and compliance [9,18,20,22,24,29].

The literature, therefore, indicates that the role of RPA in auditing and fraud control is primarily to improve the efficiency and effectiveness of audit engagements and automating evidence gathering and analysis to allow for wider audit scope and therefore an increase the ability to detect fraudulent activity. RPA can allow for standardizing, documenting and speeding up of audit engagements and high-risk activities and can aid auditors in performing their duties.

Furthermore, RPA can be used outside of the audit function to standardise organizational controls and ensure adequate documentation and compliance with control requirements to reduce he opportunities for fraud to take place [27,29].

3.2 Process Identification for RPA

The literature analysed, indicates that there is no consensus on which activities should be automated by robotic process automation. However, there is a need to automate processes which are highly structured and repetitive in nature [7,10,13,15,17,19,22,25], although the specific functional areas or tasks are not specified [13].

In other words, structured audit tasks which are well defined are best suited to RPA automation techniques [22,25], such as substantive audit procedures [10]. Expert involvement is required to identify which processes can be automated and how to optimise the solution [15, 17]. Understanding how to automate the processes is equally as important as identifying the processes for robotic process automation [10,19].

An example from the literature is the use of robotic process automation to automate substantive procedures testing loan valuation, recording and disclosure [10]. Data was collected from source reports, prepared for loading into Microsoft Access and automatically execute the desired audit tests [10], where it was able to detect the expected anomalies faster than an auditor could [10].

Processes are identified for automation based on task data structure and repetitive, predictable workflow. RPA is sometimes classed as part of the wider intelligent process automation (IPA) environment [7,15,21,25]. This means that RPA could potentially be integrated with other intelligent automation tools such as tools that involves machine learning [22] to further enhance its effectiveness [25-26].

Also note that RPA automate existing processes rather than replacing them and may therefore automate existing control weaknesses and inadequacies [18]. While RPA does not necessitate process reengineering [24], it could perhaps be a driver of audit engagement and fraud control improvement to enable its use [19].

3.3 Data Standardization

RPA requires quality data to perform adequately [13]. When a robotic process automation solution is being considered, the format, source and compatibility of related data must be considered [7,15].

In the literature, there are two dimensions to data standardization. First, organizations that implement RPA need to consider cross-functional organizational data needs [20] and their related controls [13]. Furthermore, organizations which aim to reduce fraud using RPA should ensure that the data needed is of the correct level of detail,

quality and security [13]. Just as RPA can cause incorrect decision making if implemented with poorly designed process, poor data and data standards can lead to similar problems.

The second dimension for data standardization is audit data standards. In order for RPA software, when used by the audit function, to give consistent and reliable results, the data dictionary, labels and preparation methods for auditing should be defined and followed by the audit function [10,15].

To conclude, the successful use of RPA in organizations to address fraud and enhance audit interventions require strict data standardization and governance considerations.

3.4 RPA Vendors

In the literature, a number of articles refer to specific vendors for implementing RPA solutions [14,15,19,22,25]. Only one literature source mention the development of in-house RPA solutions [15].

In other words, in-house development for audit and fraud control RPA systems does not appear as widespread as vendor-provided solutions. It further appears that RPA solutions developed in-house may be used in conjunction with vendor purchased solutions to address fraud and audit control needs in an organization [15].

3.5 The Changing Role of the Auditor

As mentioned earlier, one of the roles of RPA in auditing and fraud control is the replacement of mundane tasks, allowing employees to focus on more challenging, value-adding tasks.

This implies that the role of auditors will change to better fit the new role demands that RPA offers. Data analytics is one area that is transformed when using RPA [25]. RPA allows for more data to be collected and processed than if similar processes had to be conducted manually [25]. Data can also be analyzed in conjunction with other artificial intelligence technologies [25]. Auditors will therefore need a good understanding of analytics and artificial intelligence techniques in order to achieve the best results from the use of RPA. This is aligned to the claim that accountants will be required to develop more technical skills for the RPA environment, such as data management [26]. The call for technical skills development in accounting students [23,26] indicates the need for professionals in this environment to embrace changing technological needs in the audit and accounting space.

The fact that RPA tools can flag suspicious transactions or records [8,12,21,23,26] for examination by experts means that a greater emphasis will be placed on professional judgement [8,10]. Auditors will need to be able to interpret flagged records adequately which may require fraud examination, analytical or forensic investigation perspective [8,23]. This perspective and professional expertise cannot be automated like the more structured, well-defined tasks which RPA targets [10]. The need for auditors will, therefore, not be significantly impacted by the use of RPA, especially considering the increased scope of audit engagements which RPA enables [25].

There is further no consensus on what the more challenging tasks undertaken by employees and auditors will be. The literature only indicates that analysis and more

challenging tasks (because of the automation of mundane tasks) will be a focus for auditors and that professional judgement and technical skills will be required. As more audit and accounting professionals develop their IT skills, in-house solutions could become more common. This points to a convergence of IT and audit principles and skills.

3.6 RPA Threats

RPA has implications with regards to governance, control and risk management in the organization.

Firstly, governance strategies of organizations will either need to incorporate RPA directly into existing governance frameworks, or create new separate decentralized RPA-specific governance structures to address the organizational changes brought about by RPA [13]. In either case, governance structures should be in place before any RPA implementation takes place [21].

Secondly, risk management strategies need to consider the effects of RPA [23]. Processes and process constraints may not be automated correctly in RPA software, which may lead to incorrect process results and unexpected process exceptions that carry risk [22]. Privacy and security concerns also affect the risk environment. Digital evidence gathering during auditing may potentially exposes sensitive data [15, 22]. In other words, there may be an increase in the risk of organizational cybersecurity breaches. These risk areas will require adjustments to the risk register of the organization and may lead to the modification of auditing standards [8].

Changes in governance and risk will further necessitate changes to the control environment. In order to address the security risks created by using RPA, controls will need to be implemented which aim to mitigate those risks. The organisation should implement controls which ensure the confidentiality, integrity, accessibility, accountability, authenticity and reliability of data used by the RPA software [24]. There should also be controls which address the possibility of faulty RPA workflow [12]. With these new controls in place, there will also be a need to audit the RPA system itself [12,23] to determine their adequacy and effectiveness.

Another problem posed using RPA in audit and fraud control is the use of RPA by fraudsters. Robotic process automation may be abused by its users to more easily commit fraud [16]. The relationship between RPA and fraud still needs to be thoroughly investigated [16].

However, implementation of RPA in the process of disclosing information constituting a banking secret to authorities was found to mitigate the risk non-compliance in areas such as protection of information and meeting statutory obligations [24]. Robotic process automation may therefore also provide a means to address some compliance threats by reducing errors in critical processes.

Organizations need to consider various applications of RPA and the effects on the organizational governance, risk and control environment to ensure strategic goals are met.

4 An RPA Implementation Framework in Audit and Fraud Control

From the systematic literature review analysis and discussion, seven pre-conditions were identified (derived from Section 3) when implementing RPA for fraud control and

auditing. A discussion of these pre-conditions follow, after which an implementation framework for RPA in auditing and fraud control is proposed.

4.1 Pre-Conditions for RPA in Auditing and Fraud Control

Seven pre-conditions (in no particular order) were identified for the successful implementation of RPA in fraud control and auditing. These pre-conditions may serve as a checklist that organizations may use for implementing RPA in fraud control and auditing.

Definition of Expected Outcomes: An organization should have a clear vision of the goals, objectives and role of a RPA implementation project. If there are clear goals, objective and roles defined for RPA in the target environment, appropriate decision of the correct processes can follow, assisting in successful implementation [10,19,22,25]. After implementation, the design can be evaluated against the defined goals, objectives and roles for RPA in the organization.

Structured Processes: A successful RPA implementation initiative requires that processes are already well structured and meet organizational goals [10,18,22,25]. Furthermore, processes targeted for RPA projects or engagements should already be well optimized and fit for purpose.

Involvement of Experts: The RPA solution should be implemented through collaboration with experts. This includes process experts who understand the process being automated, audit and fraud experts who can guide the project regarding control best practice, as well as information technology experts who can provide insight into the data and technical environment [8,10,15,17,19].

Data Standardisation: RPA requires structured data to perform adequately, therefore it is necessary to standardize data [22,25]. As consequence, if a RPA solution is implemented in a fraud control context, cross-functional data is available [20] which will be well understood and can be leveraged easily. If the RPA solution is being implemented in an audit context, then data standardization also refers to the audit data standards which should be in place to ensure consistent, easily interpreted results [10,15].

Evaluation of Threats: An evaluation of the threats which may occur in the target environment should be conducted. The changes which may occur in the governance, risk and control environment of the organisation as a result of a RPA solution being implemented [12,13,15,22,24] should be taken into consideration so that they can be responded to appropriately [21].

Solution Procurement: Organizations should decide whether a vendor RPA solution will be purchased, or an in-house solution will be developed, or a combination of both [15]. The type of solution which will be used may affect the time, cost, skill requirement and quality of the RPA project [14,15,19,22,25].

Skill Requirements: An organization need to determine whether or not it has the necessary skills to successfully implement a RPA solution. There will be a need for process, audit and IT experts [8,23,25,26], which may not be present in the organisation. If an in-house solution is required, there will be a need for RPA developer skills [15]. These skillsets are needed to successfully implement a RPA solution which meets the organisational goals.

4.2 An Implementation Framework

An implementation framework for RPA in auditing and fraud control is proposed that combine the identified literature themes of this study. The proposed framework involves the phases of *Process Identification* [7,10,13,15,17,19,22,25] , then *RPA Design and Construction* (and the technical skills involved) [23,26] and finally the *Results Evaluation* (or analytics) [25] presented by the software (see Fig. 1).

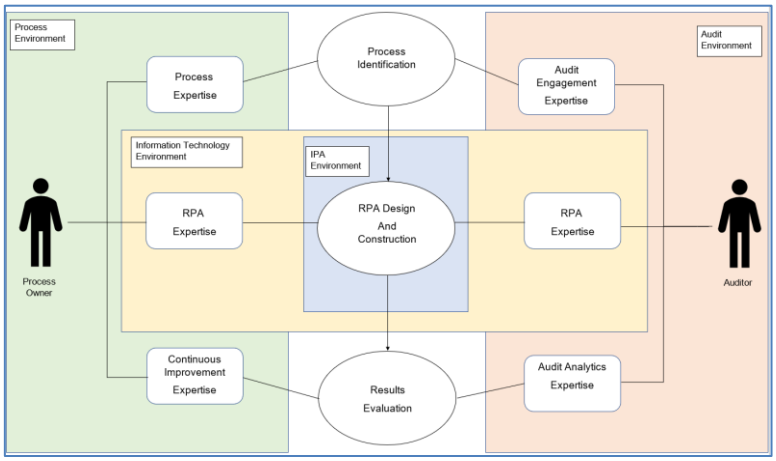

Fig. 1. An Implementation Framework for RPA in Auditing and Fraud Control

The RPA pre-conditions for auditing and fraud control (Section 4.1) may assist to prevent and detect fraud. These pre-conditions apply to both the audit environment and the existing process environment. In the audit environment, it is at least the auditor who will need to consider these pre-conditions and on the process environment, it is at least the process owner, as illustrated in the proposed implementation framework.

Process identification involves the identification of processes which are best suited for automation to meet organizational or audit engagement objectives. These are typically simple and structured tasks whose output is needed for later tasks [7,10,13,15,17,19,22,25].

The framework considers the design and construction of the RPA solution to be a part of the organization's intelligent process automation environment [7,15,21,25]. The organization implementing the RPA solution, should consider RPA within the context of any existing IT and intelligent process automation strategy.

The framework considers results evaluation to be any usage of the output of the RPA system to determine the existence of fraud and how best to prevent it from occurring in future.

The three high-level phases described in the framework involve various skills which are needed for the implementation of RPA. The skills will also differ between the process and audit environments.

The first phase, *Process Identification*, requires identifying processes for automation that requires process and audit expertise in the context of that specific process environment.

The second phase, *The RPA Design and Construction*, requires RPA development expertise, regardless of the environment the automation takes place in.

Lastly, *Results Evaluation* of the automated process will either cause changes to the implemented process to further reduce fraud in the process environment, or be used in audit analytics in the scope of the audit engagement.

This research confirms the cross-functional overlap in skills that is required for RPA implementation in the audit and the information technology environments [23,26], as indicated in Figure 1. There is no guarantee that all of the required skills will exist in an organization therefore, organizations should hire or contract in these skillsets and necessary RPA software when needed [14,15,19,22,25].

5 Conclusion

This systematic literature review has recognized a total of 22 articles that explain how RPA may offer ways for organizations to reduce the risk of fraud and advance audit effectiveness.

The content from the chosen articles were organized into six distinct themes that describe the role of RPA in auditing and fraud control.

These themes are: process automation - reducing the time spent by auditors and employees on mundane, repetitive tasks that allow for greater focus on challenging and value-adding tasks; the changing role of the auditor – proposing an expansion of auditor skills to include more technical skills required to make best use of RPA in auditing and fraud control; RPA vendors – that indicate most organizations make use of RPA vendors with the necessary skills and expertise to implement RPA solutions rather than embarking on in-house development; RPA threats – RPA implementations have an impact the governance, risk and control environment of organisations; process identification for RPA - processes automated identified for RPA should be structured or semi-structured in nature; data standardization - the successful use of RPA in organizations to address fraud and enhance audit interventions require strict data standardisation and governance considerations.

Finally, this review contributes to the body of knowledge by presenting a list of preconditions for the successful use of RPA in auditing and fraud control. Furthermore, a RPA implementation framework was proposed, that organizations, practitioners and researchers may consider in audit and fraud control environments.

6 References

1. Association of Certified Fraud Examiners. Global Study on Occupational Fraud and Abuse Report to the Nations **10** (80), (2018).
2. Association of Certified Fraud Examiners. https://www.acfe.com/rttn2016/images/fraud-tree.jpg (2019).
3. Nia, E. H., Said, J. Assessing Fraud Risk Factors of Assets Misappropriation: Evidences from Iranian Banks. Procedia Economics and Finance **31**(15), 919–924 (2015).
4. Suh, J. B., Nicolaides, R., Trafford, R. The effects of reducing opportunity and fraud risk factors on the occurrence of occupational fraud in financial institutions. International Journal of Law, Crime and Justice **56**(January), 79–88 (2019).
5. Petraşcu, D., Tieanu, A. The Role of Internal Audit in Fraud Prevention and Detection. Procedia Economics and Finance, **16**(May), 489–497 (2014).
6. van der Aalst, W. M. P., Bichler, M., Heinzl, A. Robotic Process Automation. In Business and Information Systems Engineering **60**(4), 269–272 (2018).
7. Huang, F., Vasarhelyi, M. A Applying robotic process automation (RPA) in auditing: A framework. International Journal of Accounting Information Systems **35**, 100433 (2019).
8. Appelbaum, D., Nehmer, R. The Coming Disruption of Drones, Robots, and Bots: How Will It Affect CPAs and Accounting Practice. The CPA Journal **87**(6), 40–44 (2017).
9. Asquith, A., Horsman, G. Let the robots do it!-Taking a look at Robotic Process Automation and its potential application in digital forensics. Forensic Science International: Reports (2019).
10. Cohen, M., Rozario, A., Zhang, C. Exploring the Use of Robotic Process Automation (RPA) in Substantive Audit Procedures. The CPA Journal **89** (7), 49–53 (2019).
11. Hale, A., VanVleet, E., Butt, J., Hollis, T. The "Power of With": Combining humans and machines to transform tax. *International Tax Review*, N.PAG-N.PAG (2020).
12. Kaya, C. T., Turkyilmaz, M., Birol, B. RPA Teknolojilerinin Muhasebe Sistemleri Üzerindeki Etkisi. Muhasebe ve Finansman Dergisi **82**, 235–250 (2019).
13. Kokina, J., Blanchette, S. Early evidence of digital labor in accounting: Innovation with Robotic Process Automation. International Journal of Accounting Information Systems, 100431 (2019).
14. Madakam, S., Holmukhe, R. M., Jaiswal, D. K. The Future Digital Work Force: Robotic Process Automation (RPA). Journal of Information Systems and Technology Management **16**, 1–17 (2019).
15. Moffitt, K. C., Rozario, A. M., Vasarhelyi, M. A. Robotic process automation for auditing. Journal of Emerging Technologies in Accounting **15**(1), 1–10 (2018).
16. Nickerson, M. A. Fraud in a World of Advanced Technologies: The Possibilities are (Unfortunately) Endless: Certified Public Accountant. The CPA Journal **89**(6), 28–34 (2019).
17. Osman, C.C. (2019). Robotic Process Automation: Lessons Learned from Case Studies. Informatica Economica **23**(4), 66–75 (2019).
18. Raju, P., Koch, R. Can RPA Improve Agility. Strategic Finance **100**(9), 68–69 (2019).
19. Rozario, A. M., Vasarhelyi, M. A. (2018). How Robotic Process Automation Is Transforming Accounting and Auditing. The CPA Journal **88**(6), 46–49 (2018).
20. Shroff, M. How Intelligent Finance Decodes Data. Treasury & Risk, 1–4 (2020)
21. Steinhoff, J., Lewis, A., Everson, K. The March of the Robots. The Journal of Government Financial Management **67**(1), 26–33 (2019).
22. Syed, R., Suriadi, S., Adams, M., Bandara, W., Leemans, S. J. J., Ouyang, C., Ter Hofstede, A. H. M., Van De Weerd, I., Wynn, M. T., Reijers, H. A. Robotic Process Automation: Contemporary themes and challenges. Computers in Industry **115**, 103162 (2020).

23. Tucker, I. Are You Ready For Your Robots? Strategic Finance **99**(5), 48–53 (2017).
24. Wojciechowska-Filipek, S. Automation of the process of handling enquiries concerning information constituting a bank secret. Banks and Bank Systems **14**(3), 175–186 (2019).
25. Zhang, C. Intelligent process automation in audit. Journal of Emerging Technologies in Accounting **16**(2), 69–88 (2019).
26. Lin, P., Hazelbaker, T. Meeting the Challenge of Artificial Intelligence: What CPAs Need to Know. The CPA Journal **89**(6), 48–52 (2019).
27. Hradecká, M. Robotic Internal Audit-Control Methods in the Selected Company. AGRIS On-Line Papers in Economics and Informatics **2**(2), 31–42 (2019).
28. Madakam, S., Holmukhe, R. M., Jaiswal, D. K. The Future Digital Work Force: Robotic Process Automation (RPA). Journal of Information Systems and Technology Management **16**, 1–17 (2019)
29. Ferreria, C., Serpa, S. Society 5.0 and Social Development: Contributions to a Discussion. Management and Organizational Studies **5**(4), 26-31 (2018).
30. Potocan, V., Matjaz, M., Nedelko, Z. Society 5.0: Balancing of Industry 4.0, Economic Advancement and Social Problems. Kybernetes 50(3), 794-811 (2020).