The Impact of Implementing Robotic Process Automation (RPA) on the Internal Audit Function: A Malaysian Study

Ng Li Xin*[a], Kannan A/L Asokan [b], Suresh A/L Balasingam [c]
[a] Research Scholar, Asia Pacific University, Malaysia
[b] Lecturer, Asia Pacific University, Malaysia
[c] Senior Lecturer, Asia Pacific University, Malaysia
*Corresponding author Email: *lixin.yzz@gmail.com

Abstract

Robotic Process Automation (RPA) is gaining popularity in the business environment. New technology imposes new risk concerns, its nature of imitating human interaction has challenged the auditing process, resulting in a new skillset required by the internal auditor to tackle the issues. This study provides an overview of the impact of implementing RPA on the Internal Audit Function (IAF) in three areas: key risks within the RPA implementation, the changes in the internal audit processes and the skillset required by the internal auditor. The results are observed through interview with practitioners from the field of internal auditing, IT auditing and RPA. The study used a purposive sampling technique to select target respondents required for the semi-structured interview, a total of nine participants are selected as the sample size for the study based on their experience and basic knowledge in internal auditing or RPA development. The findings revealed that the implementation of RPA have a significant impact on the IAF by introducing new risks, transforming the internal audit process, and demanding new skillset of internal auditor. This study contributes to the literature in internal auditing in general, and in IT internal auditing more specifically. This study also responds to the recent call for insightful research in RPA.

Keywords: Robotic Process Automation; RPA Risks; Internal Auditing; IT Internal Auditing

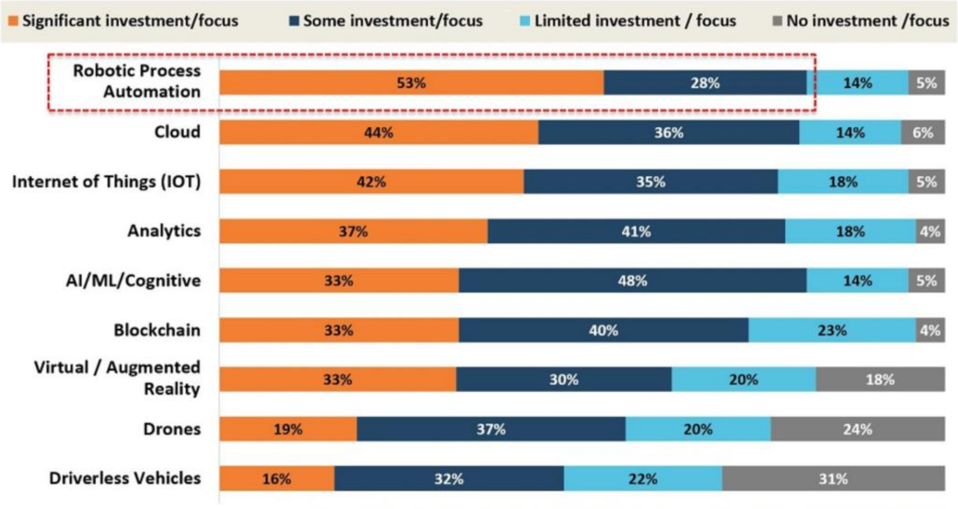
1 Introduction

In recent years, the business world is facing with emerging challenges and developments. With the growing shift toward complexities, businesses experienced challenges in handling technological, economic, and social developments (Kaya, et al., 2019). Businesses are now revolutionizing their way of operating and expanding, driven by Industry 4.0 (Epicor, 2020). The Fourth Industrial Revolution emphasize on the improvement in digital technology with the help of **interconnectivity**, **machine learning**, **real-time data,** and **automation**. Industry 4.0 advances the trend of automation through digitization and linked production, making Robotic Process Automation (RPA) one of the key elements driving companies from Industry 3.0 to 4.0. RPA is one of the core technologies within Industry 4.0 that will fundamentally amend the infrastructure and processes of both back-end and front-end enterprises to significantly reduce cost, increase production, provide a better quality of output and lead to a higher customer satisfaction.

“They say nobody can buy time. We challenge them.” – Slogan of an RPA technology provider - Aggranda (2020).

Using a computer or “virtualized robot” rather than a person to manipulate existing application software, RPA is the application of specific technology and methodology to claims applications, databased, learning management systems precisely like a person today processes a transaction or completes a process (Madakam, et al., 2019). RPA is also known as a preconfigured programme that uses business rules and predefined activity choreography to complete the autonomous execution of a human exception management outcome or service in one more unrelated software systems. In short, RPA, the bots automate human tasks (Moffitt, et al., 2018).

According to the market research report published by P&S Intelligence (2020), the global RPA market is expected to grow from around $1.6 billion in 2019 to about $46.0 billion by 2030. It is believed that with swift digitization, companies across numerous verticals are implementing virtual workforces, as RPA helps automate the business process, thereby saving time and operational expenses. In addition, research conducted by Horses for Sources (HfS), in conjunction with KPMG, RPA is voted as the top of investment of organizations to achieve operational cost saving goals (Fersht, 2018). Thus, it can be seen that RPA occupies one of the important strategies for the development of organization.



Source: HfS Research in Conjunction with KPMG, "State of Operations and Outsourcing 2018, March, 2018
Sample: (Interim Data) Enterprise Buyers (Global 2000) = 250

Figure 1. RPA, Cloud & IoT Lead Investment Focus

For organization exploring the opportunities of RPA, continuous improvement and automation are their strategic goals. RPA has gained more attention in recent years compared to other technologies, such as Artificial Intelligent (AI) and Machine Learning (ML). It is because RPA is usually low-cost and easy to incorporate relative to expensive AI and ML solutions. RPA is usually non-intrusive, without creating significant disruptions, it can quickly fit within the existing IT infrastructure and give organization a return faster than other technologies (Chau, 2019). History has shown that automation tends to create more jobs than it demolishes, as human skills become more crucial in monitoring, decision making, interpreting results, and providing insight and service to customers. In essence, RPA empowers employee to increase their individual worth and value, and fully interact with the purpose and strategy of their organizations (Fersht, 2018).

Malaysia has introduced a National Data and AI policy by mid-2020 to locate itself as a platform for AI talent grooming in South-East Asia, and to support its efforts in constructing commercial AI ecosystem (Globaldata.com, 2020). The development of Malaysian RPA Center of Excellence (CoE) further support and accelerate customer adoption of RPA in Malaysian workforce. This CoE is collaborated by Capgemini, a global digital transformation consultant, and Blue Prism, one of the biggest RPA developers and vendors. As a result, there will be more local talents to be prepared for the digitalized workforce in Malaysia (Tan, 2019). It is also reported by The Edge Markets Malaysia, other than large companies, Small and Medium-sized Enterprises (SMEs) are now better positioned to implement new technologies given the affordable cost of deploying RPA. RPA assists SMEs in scaling more sustainably and enabled them to be more flexible in dealing with unexpected incidents, such as COVID-19 pandemic (Amirudin, 2021).

In finance, accounting, human resources, shared services and other areas of organizations where the processes and procedures are stable, repeatable and high volume, RPA is prevalent. A value-based and business-focused RPA strategy enabled organizations extract 25-200% Return of

Investment (ROI) from this digital transformation. Consequently, audit leaders need to understand and consider the associated threats and opportunity that RPA could brought to the Internal Audit Function (IAF), the third line of defense itself. Internal auditing is facing challenging in providing reasonable assurance over many newly automated processes, the teams should conduct RPA governance reviews to provide assurance over organizational RPA implementations (Bryan, 2019). The internal audit profession must see emerging technology from the perspectives how the technology would affect its position. There are many aspects of process automation that can contribute to increased risk exposure as compared to a traditional IT application. As a result, control design of a company's internal control needs to be evolving with the RPA implementation in an organization. As the business adopts technology in their control organization-wide, internal auditors have to consider new or heightened risks that this may present and how they can provide assurance against these risks (PwC, 2017a).

At the same time, the importance and the mission of the IAF evolves as regulators seek better ways to protect investors, consumers, and businesses; while board members and senior executives look for better ways to protect their interests as well as those of the organizations and stakeholders to whom they are accountable (Gray, 2016). RPA brings both **responsibilities and opportunities** to internal audit. In the first place, IAF as a trusted advisor and need to collaborate with other leaders on ways to enhance the control environment as business processes are redesigned and automated using RPA. Within internal audit, new testing approaches will be needed for automated processes (PwC, 2017a). The forthcoming data ecosystem will consist of a large chain of interlinked data sources and many constantly acting intelligent agents performing assurance tasks and drawing exceptions in some form of continuous audit (European Court of Auditors, 2020). IAF that are relatively advanced in their use of data analytics would easily manage to build continuous auditing system. For example, when RPA is established to automate the extraction and transformation of the data from a source system, the audit tests can easily be re-run on a regular or continuous basis (PwC, 2019).

As RPA momentum increases, internal audit professionals must keep pace by helping company understand and control RPA risks and beforehand embracing RPA within their own organization. IAF as the control functions should make sure control standards are in place for the roll-out and management of RPA. Thus, this study explores the impact of implementing organizational RPA on the IAF in three areas: key risk areas within RPA implementation, changes in the internal audit process and lastly, the skillset required by the internal auditors.

1.1 Problem Statement

In 2016, KPMG and Forbes conducted a survey that aimed more than four hundred Chief Financial Officers (CFO) and audit committee chairs to discuss towards the developments of internal audit, and 90% of the respondents declared that their IAF is not adequately identifying and responding to emerging risks. They commented internal audit needs to be more proactive in identifying and mitigating risk, not just assessing the controls already in place. The use of technology, data and analytics in audit approach and methodology undoubted become the biggest challenge for internal auditor (Chuah & Maes, 2016). Over the years, the development of automation has been increasing the impact on IAF. Many issues should be considered on how IAF caped with the RPA implementation. RPA and its use expand, IAF cannot help but face formerly human-controlled processes that are new performed robotically. Within the next few years, internal auditor is increasingly likely to encounter RPA in routine audit engagements.

As RPA is a recent topic, the literatures do not synthesise the main topics related to the effect of RPA on the IAF. The study of Duncan & Whittington (2016) introduced the risks and issued on cloud computing might threaten IAF. The literature identified the cloud issues and its impact on compliance. Moorthy, et al. (2011) also presented the risks posed by Information Technology (IT), and how internal auditors should tackle modern information and technologies. ***Hence, what are the key risk areas within RPA implementation in organizational-wide?***

RPA allows IAF to move beyond traditional detective or preventative methodologies of periodic artifact request. Prior study by Moffitt, et al. (2018), they addressed various research opportunities towards the implementation of RPA in internal audit, provided new assurance processes should be created. While Ernst & Young LLP (2018) highlighted the role of internal auditor to be better prepared for impacted on the audit plan and consider a new process affected by RPA. However, this topic has not yet been clarified and empirically tested. ***Thus, the second question will be, what would be the changes in the internal audit process for organizations undertaking RPA?***

Existing research has so far explored the use of RPA, particularly in the field of accounting that required mandate tasks and some of the challenges and opportunities involved (Cooper, et al., 2019). Other study such as findings of Lois, et al. (2020) draw the attention of internal audit to the skills and training for the establishment of an effective auditing system in digital era. However, a focus overview on skillset expected by IAF for the organizations implemented RPA has been missing so far. ***Therefore, what are the skillset required by internal auditors?***

IAF as the third line of defense that provides independent, objective assurance over an organization’s risk management, internal control, governance and the processes in place for ensuring effectiveness, efficiency and economy. Implementation of RPA brings both responsibility and opportunities to the IAF to design an audit plan that keep pace with the emerging technologies. Thus, this study is conducted to explore the impact of implementing RPA on the IAF. Early participation of IAF in an RPA initiative ensures a balanced discussion, risk assessment and consensus on the overall structure for governance and process design.

1.2 Research Objectives

This study aims to provide an overview of an organization’s Internal Audit Function to keep pace in the era of Robotic Process Automation. The specific objectives presented as follow:

i) To explore the key risk area within Robotic Process Automation implementation in an organization.

ii) To understand the changes in the internal audit process for organizations undertaking Robotic Process Automation.

iii) To understand the skillset required by internal auditors.

1.3 Research Questions

The research questions are presented as follow:

i) What are the key risk areas within Robotic Process Automation implementation in an organization?

ii) What are the changes in the internal audit process for organizations undertaking Robotic Process Automation?

iii) What are the skillset required by internal auditors?

1.4 Significance of Study

(1) Theoretical contribution

This study explores the impact of organizational RPA implementation on the IAF. This study is contributed as a basic review and it provides more comprehensive knowledge to the researcher and student in the internal auditing area to keep pace with the Industry 4.0, and specifically in terms of RPA.

(2) Academic contribution

This study’s goal is designed to help the academic institution and accounting and auditing students to improve academic competence and provide an empirical review of the impact of RPA implementation on the IAF. Furthermore, it is significant to researchers who are concerned with doing further research by creating paths to focus within this spectrum of study.

(3) Managerial contribution

Data given will provide internal auditors with information on what is the impact of the organization adoption of RPA on internal auditing, specifically the key risk area, changes in the internal audit process and skillset required within an RPA implementation, through this study. The results will enable internal auditors to take more consideration in designing a control framework in planning annual audit and so forth. This finding also assists the internal audit industry to understand how to cope with the new technology adoption in organizations.

1.5 Scope and Limitation of the Study

This study is concerned with implementation of RPA in the organizational-wide and the impact on the IAF as the third line of defense. This study aims to explore the relationship between the adoption of RPA in organizational-wide and its impact on IAF. RPA was chosen as the research topic as its special characteristics that raised consideration of internal auditors. Specifically, it addresses three independent variables namely key risk areas, changes in the internal audit processes, and skillset required by internal auditors. The research focuses only on the internal auditing, the third line of defense as the dependent variable. This is a qualitative research study conducted through primary data and interview. For the collection of data, interview questions are open-ended questions and nine practitioners from the field of internal auditing, IT auditing and RPA developers in Malaysia will be selected for the interview.

The study is only focus on the impact of organizational implementation of RPA on the IAF, given the uniqueness of the IAF as the third line of defense that aimed to provide reasonable assurance on the new technology. As the time moving on, further research can be conducted in the topic of how IAF should adopt RPA in terms of improve internal audit efficiency and so forth.

The duration of this study is relatively short. This research is being conduct for seven months only from August 2020 to March 2021 which the information may not be absolutely up to the latest date. The only eight months duration also insufficient for the researcher to investigate more deeply and broadly into this study. Next, as RPA is relatively new and evolving, finding the relevant journals and previous research is difficult as there is paucity of research dig into this topic, especially in terms of auditing the RPA. Besides, a time series of 2015 to 2021 for articles and journals is selected. The availability of the data is also limited as the information need to be remained confidentiality.

1.6 Operational Definitions

Table 1: Operational Definitions

Terms	Definitions
Robotic Process Automation (RPA)	RPA is a software that interacts with other application software at the user interface level and is used to automate processes that are structured and rule-based (Cohen, et al., 2019). No physical robots will be discussed in the context of RPA. Also referred to “bot”, “software robot” in this study.
Automated environment, RPA environment	An automated environment in this study refers to a business environment where the processes, operations, accounting are carried out by RPA.
Robotic Process Automation Developers	An RPA developer is a technical enabler who design, built and implement a bot. He/She is came to the role with programming skills and knowledge in programming control

	flows, exception handling, and data structures (Carr, 2020).
Robotic Process Automation Consultants	An RPA consultant, also referred to RPA analysts, is responsible for perform RPA assessment and identify opportunities for process improvement. He/She is served as an integrator between business and technology, and design RPA strategy to satisfy the business needs of clients (Carr, 2020).

2 Literature Review

This chapter reviews and discusses the literature and past research in the area of RPA and internal audit. The chapter will outline the theory grounding of the study, followed by a review of the internal audit, RPA, RPA risks, audit processes and skillset of internal auditors. Literature gaps also will be identified.

2.1 Conceptual Framework

A conceptual framework (*see Figure 2*) is proposed for this study, to explore the impact of implementing organizational RPA on the IAF. According to Miles, et al. (2014), a conceptual framework is a system of concepts that communicates and explains relationships among the key factors, concepts or variables. This study adopts the IIA's Three Lines of Defense (3LOD) model into the conceptual framework and clearly visualizes the relationships among the three variables: key risk areas within RPA implementation, changes in the internal audit process and skillset required by internal auditor.

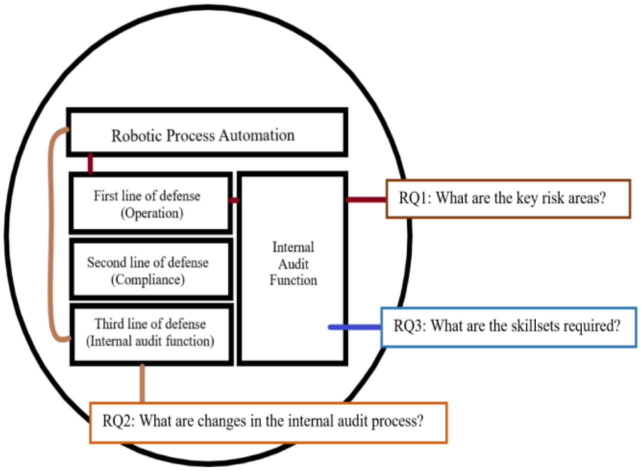

Robotic Process Automation
First line of defense (Operation)
Second line of defense (Compliance)
Third line of defense (Internal audit function)
Internal Audit Function
RQ1: What are the key risk areas?
RQ3: What are the skillsets required?
RQ2: What are changes in the internal audit process?

Figure 2. Conceptual Framework

3LOD organising essential roles and duties into three levels or "lines of defense", to enhance the clarity of risks and controls and help improve the effectiveness of organization's risk management. The first line of defense comprises the risk-owning functions, and the second line comprises functions that are responsible for enforcement and oversee the risk management. The third line is IAF itself, which offers independent assurance (IIA, 2013).

3LOD model is widely used in a risk management. The three lines of defense explains roles and duties of risk management. According to model, the three lines are necessary to facilitate the risk management and internal control (Kovanen, 2020). The IIA (2018) acknowledges that the 3LOD model needs to keep up with the emerge changes in market conditions and technology shifts in a virtual and networked world. As per this study, RPA is disrupting the business processes that mainly carried out by the first line and second line. As a result, the third line must therefore similarly incorporate the right capabilities to remain abreast of changes and ensure they provide effective oversight and objective assurance, respectively (ICAEW, 2019).

In this study, IAF acts as third line of defense upon the implementation of RPA in the organizational-wide, it is important for IAF to address the risks, understand the changes in process and update their skillset. The research questions are presented in the conceptual framework, whereby the first research question related to the RPA implementation across the operation and it aimed to identify the key risk areas posed to the organization. The second research question discussed the direct impact of RPA to the third line of defense and it aimed to understand the changes in the internal audit process for organization undertaking RPA implementation. The third research question highlighted the implied impact of RPA to the IAF and it aimed to explore the skillset required by the internal auditors.

2.2 Internal Audit and IT Internal Audit

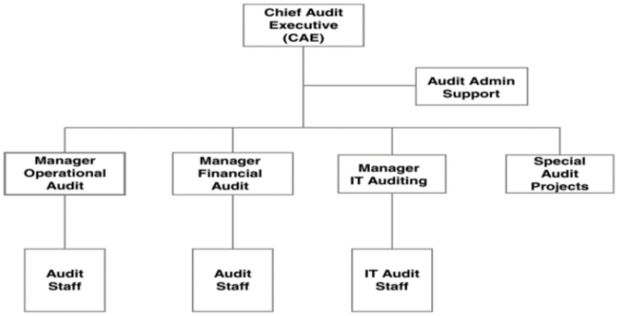
IAF is independent from the operations, that intended to add value and improve an organization's operations by providing objective assurance and consulting activity. Internal auditors use systematic and disciplined approach to evaluate and improve the effectiveness of an organization's risk management, control, and governance process (IIA, 2004). Internal auditors are regulated by International Professional Practices Framework (IPPF) ("the Standards") and the Code of Ethics. The evolving practices of internal auditing have led to the development of internal audit best practices and value added to the organization and its stakeholders by understanding the relationship between internal auditing and organizational goals. Internal auditors have now moved from a confrontational approach to partnering with management and shifting from a controls approach to a risk-based approach (Hass, et al., 2006).

Internal audit has been facing numerous opportunities risks and challenges in these few decade. Lois, et al. (2020) examine the opportunities and challenges digital era posed to the internal audit in terms of the role of technology, risks, and control consideration within the implementation of new technology, skill and knowledge needed by internal auditors and urged the development of continuous auditing. Ramamoorti and Weidenmier (2004) highlighted IT affected almost every important dimension of the IAF in terms of organizational status and charter, the scope, methodologies, and internal audit practices. They agreed that the widespread influence of IT on almost all internal audit activities designed to promote and support effective organizational governance. They also stressed the importance as recognized IT serves as both a driver in strategic direction, and an enabler in execution.

As IT used by organization is becoming increasingly more complex. By providing IT control evaluation within the framework of internal controls, the IAF would have to provide increased assurance. If IT controls are properly selected and applied on the basis of the risk they are designed to handle, then a technique to continuously monitor the efficacy and validity of IT control will provide the required assurance (Hass, et al., 2006). Virtually every IAF will have staff- and supervisor-level internal auditors with financial and operational internal audit skills. In addition, most IAF should have more level of IT audit specialists. Moeller (2010) stressed the importance of need to have a specialized IT audit function or to have regular financial or operational internal audit groups with strong IT-related technical skills. He also proposed the best practices for an internal audit organization to equipped with different specialty.

Figure 3. Specialty-Based Internal Audit Organization

In the wake of IT and business transformation and ongoing digital disruption, Information Technology Internal Audit (ITIA) appears to be unique positioned to add value and support the organization though identifying risks and guiding through the implementation of their strategies (PwC, 2017b). Nowadays all businesses rely on IT in order to complete critical operational tasks, store financial and operational data, and prepare financial and managerial reports. Given the levels of expenditures and reliance on IT, it is critical that IT resources be available and secure in order to provide accurate information (Gray, 2016). Taken into considerations of RPA, there are several important reasons to examine the involvement of internal audit in RPA (IT) audit. The first is the aforementioned importance of RPA to organizations, which results in the need for review of the effectiveness, efficiency, security, and compliance of RPA-related activities within organizations. IIA (2012) further interpreted the Standards 2110: Governance and required internal audit activity have to access whether the IT governance of the organization supports the organization's strategies and objectives. IAF plays a vital role in helping the board and executives to fulfill their IT governance responsibilities. IAF may use professional literature such as IT assurance guide published by IT Governance Institute (ITGI, 2007) to link to the Control Objectives for Information Technologies (COBIT) framework for assurance professionals (Héroux & Fortin, 2013).

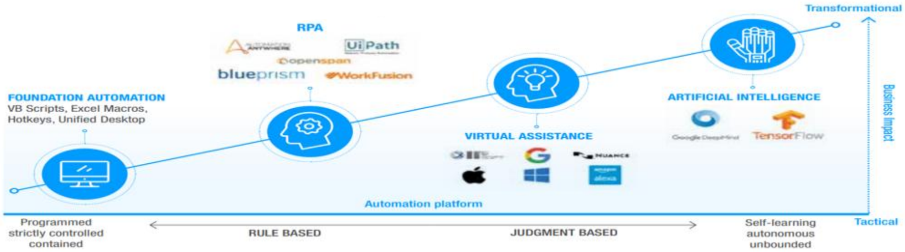


2.3 Robotic Process Automation (RPA)

Introducing Robotic Process Automation

When the technology was first developed, small scripts were written to repeat certain tasks or to provide quick integrations between system that did not have any interoperability. Over time, technology has progressed to the "fourth generation," which means that tasks that used to require many lines of computer programme can now be completed by dragging and clicking icons in a software programme (Gadre, et al., 2017).

Figure 4. RPA - Parts of a Journey Towards Machines Replacing Humans



Institute of Electrical and Electronics Engineers (IEEE) Corporate Advisory Group (2017) defined RPA as "*a preconfigured software instance that uses business rules and predefine activity choreography to complete the autonomous execution of a combination of processes, activities, transactions, and tasks in one or more unrelated software systems to deliver a result or service with human exception management.*

RPA is an emerging technology that enables anyone today to configure computer software, or a “robot” to simulate and integrate human interactions within digital systems to execute a business process. RPA robots utilize the user interface to capture data and manipulate applications just like what humans do. In contrast to traditional IT solutions, RPA allows organizations to automate at a fraction of the cost and time previously encountered (UiPath, 2017). RPA are suitable to those repetitive tasks that are standardized enough, to reduce the number of failures, and improve efficiency. In other words, each RPA has its own computer station, username and password equivalent to a human employee. The RPA marketplace is mainly dominated by three companies: UiPath Inc., Blue Prism Group PLC, and Automation Anywhere Inc (Kokina & Blanchette, 2019).

This type of automation seeks to automate business processes in order to increase the productivity while lowering costs by reducing the time spent by employee dealing with information systems, performing routine and repetitive tasks, such as typing, extracting, copying and moving huge amounts of data from one system to another systems. RPA enables employees to devote their time and resources to more value-adding tasks. RPA execute repetitive tasks by using graphical user interface (GUI) adaptors, without changing the IT infrastructure (Santos, et al., 2019; Cewe, et al., 2017). Unlike some traditional IT implementation and business reengineering that changes the existing systems, RPA tries not to disturb underlying IT systems and only replaces the existing manual process with the automated one through a presentation layer (Huang & Vasarhelyi, 2019).

Types of Robotic Process Automation

RPA has been segmented into three groups: attended automation, unattended automation and hybrid automation. Attended robots serve as a personal assistant on the user’s computer, performing a series of user-triggered actions to complete simple, routine tasks and streamline a workflow. Unattended robots required little to no human intervention to perform intensive data processing and data management. Hybrid robots are a blend of attended and unattended robots that provide user services and back-end processing in a single solution, bringing the prospect of end-to-end automated execution of complex business workflows. Organizations can incorporate all of these automation robots into a single, stable and scalable integrated automation platform, as these robots was not mutually exclusive. Organizations must develop a robust RPA strategy to choose the deployment models that best fit their needs (UiPath, 2020a).

Benefits of Robotic Process Automation

Infosys (2020) pointed three main benefits derived from RPA. RPA can lead to a higher operational efficiency by reducing the unintentional error and maintained a uniform behaviour. Low value-added processes can be eliminated results in staff effort savings. RPA can improve the compliance as the BOT has its own audit logs and transaction trails. Strict security and controls are achieved through a secure and audited robotic automation platform that is managed within an IT corridor of governance. Adoption of RPA posed a lower risk by the reduction in administrative effort.

In an automated environment, as repetitive and boring tasks that require little mental effort are automated by RPA, human employees would be freed to invest their resources in tasks that involve creative thinking, critical analysis, or social skills. In some preliminary work, software robots can support human employees, but process automation through RPA does not rely on the premise of separating and isolating individual and robots from each other but seeks to allow efficient interaction between them (Lacity & Willcocks, 2016). In this context, employee engagement, skills development, and sourcing decisions should be considered for the strategic initiatives to deploy RPA in an organization. Companies need to rethink the positions of employees because of the changing areas of responsibility (Hofmann, et al., 2020).

RPA do not require specialized programming expertise for the development software robots. A fundamental understanding of the functionalities of the information system, such as the nature of rule-based structures, the use of data, and the applications interfaces, is only required. Although the relatively low IT complexity makes RPA an easy-to-use tool in an organization for various people and functions, profound process knowledge is a decisive factor in the construction of software robot. Owing to the modularity of RPA functions and fast development cycles, employees can build new functionalities or adjust existing ones agilely. However, cooperation between business and IT functions in development and implementation of software robots is crucial as IT functions can promote the access for software robots to ERP systems (Hofmann, et al., 2020).

Requirement for Robotic Process Automation

Although RPA can benefit in cost savings, not every business process is suitable for its use. Aguirre and Rodriguez (2017), Gadre, et al. (2017) and Santos, et al. (2019) proposed some RPA-suitable process criteria:

- Rule-based tasks – RPA required process to be broken down into simple rules that are free of individual judgment, imagination and interpretation.
- Limited exception handling – RPA is ideally suited for highly standardized activities with little to no exceptions to deal with.
- Mature process – It is imperative for the process be mature because a mature process can be easily assessed, tracked, and stable to provide a better cost awareness.
- High volume – RPA automation is ideal for high-volume transactions since the high amount of repetition or time taken to complete a task is seen as a huge cost-cutting opportunity. When tasks are repeated regularly, robots can complete them faster and with lesser errors.
- Frequent interactions with multiple systems – RPA can communicate with multiple systems through the presentation layer. However, it is also notably that the system being interacted must be stable enough to avoid creating costly system exceptions.
- Human errors – Activities that are vulnerable to human error are suited for automation because it allows for cost savings and increased performance.
- Low cognitive requirements – As RPA lack of analytic and critical thinking skills, tasks that require little to no human interaction and have low cognitive requirements are suitable for automation.

Robotic Process Automation for Business Processes

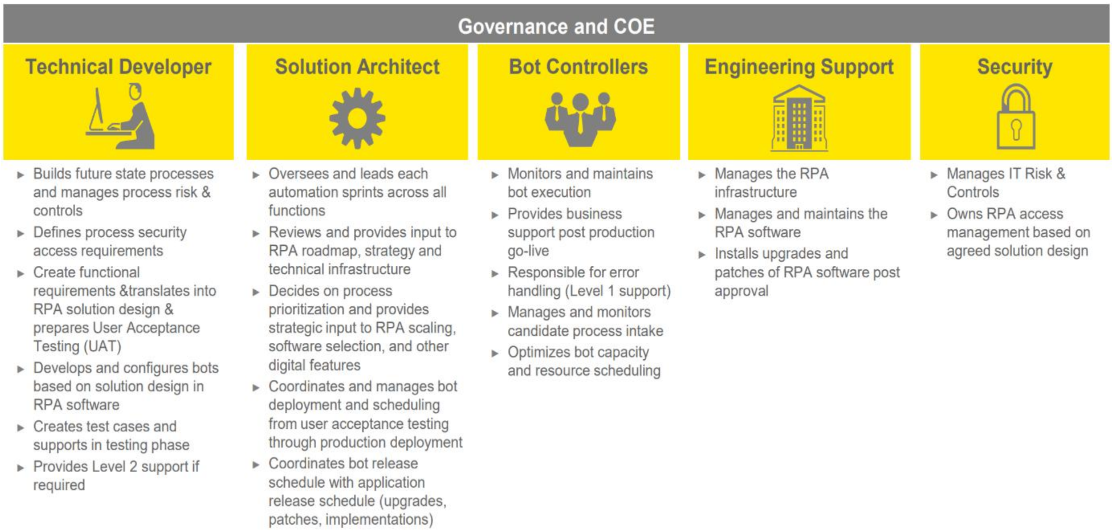
Santos, et al. (2019) proposed an approach for analysing RPA development in a business organization. They synthetized the main topics related to RPA, such as the benefits of RPA, the challenges in implementing RPA and opportunities in adopting RPA and proposed a model on the relations between the topics. The study of Aguirre and Rodriguez (2017) carried out a case study on a business process outsourcing provider on how the RPA is used in a generation of a payment receipt. They further explained the benefits and limitation of RPA.

Romao, et al. (2019) discussed the implementation of RPA in banking industry. They aimed to explores how to efficiency adopt automation in management of the most obvious process components by conducting case studies. They discussed the business process management and automation, benefits and operational risks from the adoption of RPA.

Devarajan (2018) discussed RPA's application across various industry domains. In banking industry, RPA is capable to minimize the manual processing data errors by automating customer service, accounts payables, accounts receivables, general ledger, credit underwriting, compliance, credit card processing, consumer loan processing, fraud detection, report generation and account opening or closure. In insurance industry, to cope with the rapid customer growth and improve processing time, RPA can automate manual back-office process such as claims processing, underwriting, appeals processing, data collection, policy opening or cancellation, and etc. RPA is also useful in retail industry to increase productivity by automating customer support, product categorization, marketing analysis, demand planning and monitor inventory levels. Manufacturing industries that seek for speed and scale can adopt RPA in a variety of process including bill of materials, customer service, logistics, ERP automation, data migration, manufacturing analytics and compliance process.

Robotic Process Automation Governance, Center of Excellence

On governance, Willcocks, et al. (2015) adopted various method to explore whether existing governance structures or framework could continue to match RPA decisions and management within them, and the awareness and maturity of RPA in the organizations at any one time. They concluded that, most RPA adopters manage to suit RPA within the current governance structures and framework, on the way RPA will stilly evolve the governance as it expands into new business processes and though multiple business units. In order to achieve RPA success at scale, it is essential to illuminate a long-term RPA strategy that aligned with evolving business processes and technology needs. One validated way to incorporated automation management is via a CoE. It is important to have a well-defined governance overseeing the creation and operation of bots, thus, it will provide assurance of the standard of automation, reducing risks and preventing rework (Rodrigues, et al., 2020).



Governance and COE

Technical Developer	Solution Architect	Bot Controllers	Engineering Support	Security
▸ Builds future state processes and manages process risk & controls ▸ Defines process security access requirements ▸ Create functional requirements &translates into RPA solution design & prepares User Acceptance Testing (UAT) ▸ Develops and configures bots based on solution design in RPA software ▸ Creates test cases and supports in testing phase ▸ Provides Level 2 support if required	▸ Oversees and leads each automation sprints across all functions ▸ Reviews and provides input to RPA roadmap, strategy and technical infrastructure ▸ Decides on process prioritization and provides strategic input to RPA scaling, software selection, and other digital features ▸ Coordinates and manages bot deployment and scheduling from user acceptance testing through production deployment ▸ Coordinates bot release schedule with application release schedule (upgrades, patches, implementations)	▸ Monitors and maintains bot execution ▸ Provides business support post production go-live ▸ Responsible for error handling (Level 1 support) ▸ Manages and monitors candidate process intake ▸ Optimizes bot capacity and resource scheduling	▸ Manages the RPA infrastructure ▸ Manages and maintains the RPA software ▸ Installs upgrades and patches of RPA software post approval	▸ Manages IT Risk & Controls ▸ Owns RPA access management based on agreed solution design

Figure 5: Components of an RPA CoE

Adopting Robotic Process Automation in Auditing

Few researchers discussed the opportunities of RPA with automated business process. Kokina and Blanchette (2019) explored emerging themes surrounding bot implementation for accounting and finance tasks. They measured the determinants to RPA implementation and recommended that a new understanding of risk and internal controls within an RPA implementation must be addressed by internal auditors.

Moffitt, et al. (2018) envisioned the future of audit by introducing the concept of RPA and explaining its usage in auditing. They proposed an RPA-based audits, in which the auditor’s position will be repurposed from data collector, processor, analyser, and disseminator to mainly emphasizing the assessment aspect of audit procedures. They also highlighted the benefits of adopting RPA in audit procedures where the process is repetitive and manual in nature, such as revenue testing, is best suited for automated. The researchers further brought up the consideration for an RPA-based audits, such as: reliability of RPA tools, reliability of data, privacy and security and economics of RPA.

Huang and Vasarhelyi (2019) also proposed a four-stages RPA framework for RPA-based audit. In their proposed framework, the first stage instructs auditors on how to select appropriate audit procedures for automation based on three requirements: the RPA criteria, data compatibility, and the procedure complexity. The second stage involves three steps that assist auditor in changing their current audit programme, extending the reach of the process and verifying data standardization. In the third stage, the framework suggested that auditors incorporate in-house. The last stage is to evaluate and operate the RPA-based audit procedure by evaluating the performance, assessing the detection or audit risk, and monitoring the operation.

2.4 Robotic Process Automation Risks

In accessing the additional risks posed to the organizations during the adoption of an Enterprise Resource Planning (ERP) system, Saharia, et al. (2008) highlighted the presence of the risk during the **implementation** and the **operational** stages. According to their research, organizations often facing poor project planning and control, and lacks specialized skills needed to customize the system and populate it with organizational data. Risks remain during the operational phase too, when the integrated system presents the possibility of brings down and disrupting the firm’s business operations. Despite the significant organizational risk results from an ERP implementation, involvement of internal audit to detect and mitigate potential risks appears to be critical.

Kovanen (2020) proposed that, organizations faced new challenges and risks upon the adoption of new technology. In her study, seven key risk areas were identified within the implementation of intelligent automation: risks of technology, regulatory, privacy, cybersecurity, people- and organizational-related, ethical and financial.

Some researchers have identified challenges that an organization may face after the implementation of RPA, such as robot maintenance, unclear division of responsibilities between RPA and business users, lack of understanding of RPA and expectation gaps (Santos, et al., 2019). RPA can certainly increase compliance and reduce risk. However RPA can also introduce risks if inappropriate controls are in place. RPA action is consistent, any error becomes a systemic and widespread issue across that business process and data set, it may cost a lot to the organizations. Another potential risks could be occurred such as unauthorized access gained by someone to altered or used to conduct unauthorized processing. IAF need to understand how the organization is using RPA and how that impacts its risk profile by thinking broadly about exposure across multiple categories of risk (PwC, 2017a). PwC (2017a) also established a RPA risk framework of five key categories of risks should be considered: **executive, technical, change management, operational and functional**.

Federal RPA Community of Practice (CoP) (2020) stressed seven unique risks that created along with the RPA implementation. **Rogue operators** pose a significant risk in large agencies without an enterprise-level governance structure or a formal approach for obtaining RPA services. The impact of **flawed logic and processing error** will have significant impact and contributed to one of the major key risk areas. The time and energy required to investigate, evaluate and rework processing error can create significant workloads for RPA program and staff. Internal controls experts must carefully identify risks and acceptable thresholds to determine whether the **potential liability of an error** outweighs the efficiency gain of having the automation process. RPA efforts and programs can be **complex to manage**, since they require deploying a new technology in a dynamic framework, with only limited emerging governance. The deploy of RPA may disrupt the **segregation of duties** since one individual could fill the role of developer, tester, and operator of the automation. RPA need a **proactive automation maintenance** to engage with the changes of IT system, such as system updates. Lastly, RPA created significant and enduring capacity within the organization, if issues arise with the automation, the organization may no longer have a business subject matter expert who understands the end-to-end business process to correct the issue. It consists of the risk that employees will lose the institutional knowledge associated with completing the now-automated process.

Gartner (2018) highlighted three types of risks that associated with RPA, namely business risks, governance risks and legal risks. **Business risks** included inappropriate human system integration, bot-enabled fraud, bot-enabled IT short-termism, RPA-initiated job changes and RPA overreach. Business risks is mainly introduced in business environment. **Governance risks** included RPA vendor management, RPA implementation management, RPA segregation of duties. Governance risks urged organization to develop a robust risk governance to maintain RPA. **Legal risks** included lock-in risk in which script may be incompatible between systems due to some RPA vendor usage inadvertently lock the organization into specific vendors.

Lacity and Willcocks (2017) presented eight risk categories domains surrounding PRA within organization. There are: **strategy risks, project risks, sourcing risks, operational risks, tool selection risks, change management risks, stakeholder buy-in risks and maturity risks**. While Giesbers (2020) further explain the sourcing risks, operational risks, change management risks, and stakeholder buy-in risks in the perspective of internal control, and with a focus on security and compliance. He also provided control framework based on the key risks categories in associated with internal control.

Deloitte (2018) developed the Deloitte risk management framework for RPA that presents a clear view about the types of risk which need to be considered when auditing a BOT-enabled organization. A secured and compliant RPA environment requires effective management and monitoring of the eight risk domains during the four phase of BOT implementation lifecycle. Risks of **license compliance** and **RPA strategy and governance** posed first phase of implementation which are the process screening and proof of concept. **Data leakage and privacy** and **cyber threats** need to be considered during the second phase of business case and vendor finalization. During the RPA implementation, **incident management and business continuity** and **regulatory compliance** are the top considerations for IAF. Lastly are the risks of **identify and access management** and **secured business process** at the last phase of RPA Centre of Excellent where the companies reach automation goals and reap the full value of the solution offers.

ICAEW (2018) proposed seven type of risks involved in implementing RPA: too many robots for an organization to manage, process unsuitable for automation, robots have no judgement, coding errors, malfunction of bot, damage effectiveness and robots breaks down. The researcher further explains implications of each risks as well as mitigation that internal auditor can made to reduce the risks.

Furthermore, Priyadarshi (2019) also mentioned few key risk areas that internal audit should consider when evaluating RPA implementation: misconfigured human system integration, overdone automation, tough change management, implementation gaps and mismanagement, misaligned third parties, hacking threats, cybersecurity risks and lack of security standardization for RPA. The researcher pointed out that RPA implementation usually involve process redesign or process improvement, which introducing new risks to the organizations. As organization accept new risk scenarios that come with adoption of RPA, the IAF role will continue to expand.

2.5 Internal Audit Processes

According to Rissi and Sherman (2011), depending on the type of internal audit, an internal auditor regularly reviews evidence for compliance with established criteria. The best practice in effective IT auditing is to start with an understanding of business functions, to identify which IT infrastructure is providing those functions, and to then consider the scope of the audit and controls best suited for that IT function. Bierstaker, et al. (2001) agreed the paperless audits will become prevalent where audit clients tend to shift towards paperless systems, and the internal audit operation will be relying on more audit software to enhance the auditing processes. He also noted that as companies are becoming more technically sophisticated, auditing procedures from beginning to end should discuss and direct the business process of the client and capable in measure performances.

In terms of auditing AI, Firouzi and Wang (2020) claimed that instead of audits of different teams from various areas with a lack of understanding of AI and the risks associated with it, there should be an integrated audit team with diverse backgrounds and experience on AI to concentrate on AI audits. They proposed an AI Internal Audit Framework that is corresponds to the AI lifecycle. Internal auditors were given a greater understanding of how to provide assurance on the controls affecting AI models as a result of the framework.

Moorthy, et al. (2011) then suggested the audit processes and approach may be initially targeting information for retrieval and analysis that will provide evidence of the consequences of control weaknesses where internal auditors know or suspect key control weaknesses in conducting audits of systems, information or business processes. This approach can generate evidence of the consequences of weak controls and may be a more effective use of the auditor’s time than conducting extensive analyses of the systems and control environments to identify and assess controls.

The Institute of Chartered Accountants of India (2018) raised the concern of the risks in an automated environment, whereby the risks could have impact on audit procedures in different ways. Firstly, auditors may not be able to reply on the data obtained from systems where such risk is not mitigated. All forms of data, information or reports that they obtain from systems has to be thoroughly tested and corroborated for completeness and accuracy. Second, auditor will not be able to reply on automated controls, calculations, accounting procedures that are built into the applications. Additional audit work may be required in this case. Third, the audit report also may have to be modified in some instances due to the regulatory requirement of auditors to report on internal financial controls of a company. Therefore, the auditor should be able to demonstrate how the risks were identified and what audit evidence was obtained and validated to address these IT risks. They further introduced different method for testing in an automated environment. In an automated environment, auditor may inspect the application configuration; inspect the system logs; inspect documentation of that process and carry out a test negative testing and observe error message.

KPMG (2018) pointed six areas that should be review by IAF during auditing the RPA environment. First are the **strategy** considerations. IAF should look for a clear vision of the goals and mission of the intelligent programme that shows that management recognises and supports that vision. As new servers, tools, third parties, and integration options are developed, the IAF should also consider how automation changes the overall **technology environment** and infrastructure. The IAF should access the **business process** that adopting RPA and capturing its risks and preparing to manage those risks. Intelligent automation involves improvements to **personnel’s qualifications and skill set**. In order to fulfil these needs, the IAF should assists organizations to redeploy or recruit talent. The most significantly, the IAF should identify the **financial, operational, and compliance controls** that either can be automated as part of the solution or will be affected by it. Internal audit examines procedures to verify the completeness and accuracy of all data and information processed by intelligent automation and evaluate controls designed to identify when a BOT fails to perform as it should. Finally, a **proper governance program** for the implementation of RPA should be established by the IAF. The governance activities are designed to determine if the expected benefit has been realized and continues to scale to meet the strategic business goals.

Given the specific risks arose from the deployment of RPA, Deloitte (2018) illustrated a audit process phases changes that need to be considered by the internal auditor, such as: planning, walkthrough, design evaluation, operating effectiveness and reporting. In the planning phase, a good understanding of the environment where the bot will be used must be achieved. After the auditor identifies that there are automations in an environment, a specialist with the requisite skillsets should be included in the team, right from the walkthrough stage to test the risks associated with each automation. The auditor must take due care to scope-in the bots that are directly applicable to the testing. In the case of a walkthrough of an automated environment, a code walkthrough is also essential. The auditor must decide if any exception reports are produced by the bot. Finally, the auditor needs to audit the relevant interfaces of the bot with other systems, and also familiar with the bot configuration.

Struthers-Kennedy (2018) mentioned the implementation of RPA expanded audit capabilities. RPA enabled the IAF to shift beyond traditional detective or preventive methodologies with periodic artifact requests to continuous auditing, allowing an audit cycle that could have previously taken several weeks almost instantaneous. In order to understand the processes follow to generate audit artifacts and work to automate these processes, automated artifact gathering will also allow internal audit to be more autonomous by collaborating with various departments. Generated artifacts can be stored on a routine schedule in a centralized repository and additional bots can be programmed to tick-mark evidence to assist the internal audit testing process.

In auditing RPA, Bryan (2019) also encouraged audit leader to ensure that an effective RPA programme governance system is in place and followed; related controls in RPA implementation are not inadvertently eliminated and new threats have appropriate controls in place; a transparent mechanism is in place to efficiently handle process exceptions that are likely to rise as transaction volume increases; and newly automated systems have sufficient arrangements in place to continue essential operations in case of intentional or unintentional RPA system outages.

2.6 Skillset of Internal Auditors

Competence is defined by The International Federation of Accountants [IFAC] as “being able to perform a work role to defined standards with reference to real working environment” (IFAC, 2003). In the IT environment, competence is identified as a set of IT-related knowledge and experiences that a knowledge worker processes. These competencies are imperative to enable accounting practitioners to perform their tasks (Bahador & Haider, 2015). Besides, internal auditors must only conduct services for which they have the requisite expertise, qualifications, and experience, according to Rule 4.1 of the Code of Ethics. Regulated by Code of Ethics Rule 4.3, internal auditors have to continuously enhance their proficiency, as well as the effectiveness and efficiency of their services (IIA, 2019).

In 2006, the IIA attempts to better understand the expanding reach of internal auditing practise around the world by undertaking the Global Common Body of Knowledge (CBOK) study. From the survey, in terms of **general competencies**, three common core competencies have been identified: communication skills, problem identification and solution skills, and keeping up to date with industry and regulatory changes and professional standard. In terms of **behavioural skills**, confidentiality and communication appeared to be the top core behavioural skills. In terms of **technical skills**, two core technical skills were identified: understanding the business and risk analysis and control assessment techniques. In terms of **knowledge,** risk-based audit planning and usage of CAATs were highly recognized by the internal auditors (Bailey, 2010).

Hass, et al. (2006) discussed the skillset required by the internal auditors given the expanding scope of internal auditing practice throughout the business environment. He proposed few factors that attributed to the changing requirement of the skillset of internal auditors, such as the IPPF, regulations, impact of SOX, risk assessment, increased demand on the IAF, development of IT, rise of risk-based auditing, objectivity, and strategic perspective. Then, the researcher summary his findings with a list that consists of 30 skills and competencies that required by the internal auditor.

Kovanen (2020) found that internal auditor competencies were seen as the biggest challenges internal audit when auditing intelligent automation by both, interviewees and participants in her research. She suggested auditors' competencies can be improved and maintained by training and if it is not possible or reasonable, competence gaps can be covered with different resourcing models. Internal audit should be competent in using data-analytics tools and keep up with cyber security, regulation and ethical discussion.

Pawlowski (2019) listed some emerging skillset in demand for internal auditor to make an impact at their organization in the RPA-era: skills of data science and data analytics to detect, predict, prevent and take risks, knowledge of behavioural science to understand growing popularity of behavioural economics to inform decision-making and digital literacy by utilizing systems, networks, smart devices to manage risks and controls.

There are seven concepts required by audit personnel perform the internal IT audit: communication and collaboration skills, domain and process knowledge, career development, professional skills, personality traits, technical skills and knowledge, and audit skills and knowledge that introduced in the study of Havelka and Merhout (2013). The seven concepts will directly impact the process and methodology in several ways. As a result, the level and variety of skill, knowledge, and ability of the audit personnel will enable or limit the methods used for the IT audit.

In an IT audit, IT audit skills are extensive because IT auditors must be both auditors and IT professionals. From an audit perspective, internal auditors who traditionally perform financial, operational, and compliance audits of their organizations may also need to be equipped with the IT proficiencies in the implementation, operation and maintenance of IT systems in an organization. If the IAF does not possess these skills, the IT audit may be performed by other departments, co-sourced, or completely outsourced (Abdolmohammadi & Boss, 2010).

The participants in research conducted by Cooper, et al. (2019) highlighted the importance of public accountants of having, at a minimum, an awareness of RPA. The professional now is required not only with accounting and auditing skills, it is a emerging trend for auditor to have analytical skills and be able to understand data analytics. Their research concluded that auditor with an understanding of the capabilities and RPA and computer programming experience have a competitive advantage. In addition, other skills such as cultivate critical thinking and social skills are relatively important. Given that auditor are now expected to be creative and innovative in order to solve the emerging problems.

2.7 Limitations

The studies of previous researchers reviewed in this chapter have shown the related impact of RPA implementation to the IAF. This research has identified various previous researchers' works and their ideas and findings are presented as above. However, the literature presented contains of various different opinions due to different RPA software adoption in their organizations. Also, RPA as an emerging technology is in the incipient stage, unlike implementation of ERP or cloud computing, there is lack of a holistic overview of the implementation of RPA and the impact on IAF. This research applied 3LOD model in the sense that IAF as the third line of defense is responsible for addressing the impact of RPA implementation. Furthermore, there is lack of opinion carried out by Malaysia organization or advisory firm to further investigate the implementation of RPA and the impact on IAF. More opinions in respect of this study needed to be explored. Therefore, this research is conducted to provide a best practice for IAF of Malaysian organizations to cope with era of RPA.

3 Methodology/Materials

This chapter provides an overview of the data collection method utilized to answer the research questions and to satisfy the research objectives. This chapter illustrates the presentation of research methodology featuring qualitative methods. This chapter is distinguished into several areas: research design, research sample, scope of interview, research instrumentation includes the interview questions, data analysis, and ethical consideration.

3.1 Research Design

The strength of qualitative research is its capacity to elaborate textual descriptions of how people view a research problem. Qualitative study is flexible, and it allows for more inspiration and adaptation in the researcher-participant relationship. This degree of flexibility represents the kind of understanding of the problem being pursued using the method. In comparison, a quantitative study that gathers “closed-ended” data that makes it feasible to compare responses effectively is relatively inflexible (Mack, et al., 2005).

This study is a qualitative research to understand the impact of RPA implementation on the IAF. Qualitative data, with emphasis on people’s experiences, which is well suit for this study for understanding the topic. Qualitative study provides a comprehensive overview of real-life depiction and exploration (Kovanen, 2020). This research topic is emerging in the field of accounting and auditing, as well as in research. RPA is still not widespread in the Malaysian market; therefore, qualitative research is suitable research method. Primary data is collected through interview. It is aimed to pursue in-depth information around this topic.

Practitioners from the field of internal or IT auditing and RPA in Malaysia is invited to better understand the RPA implementation and their impact to the IAF. The choice for these two categories of respondent is made, as the RPA developers has expertise in developing and implementing RPA whereas the internal and IT auditor has expertise in internal and IT auditing and could therefore assess the research in a more comprehensive view. Therefore, two sets of interview questions will be prepared based on the areas of expertise in which the auditors and RPA developers involved in. The semi-structured interview sessions are conducted with the duration of 15 to 30 minutes.

3.2 Research Sample

In a qualitative study, the sample size used is often smaller than that used in a quantitative study. A qualitative study focuses on how and why of a particular issue. In-depth interview work is not about generalizing the interest of a broader population and does not appear to focus on hypothesis testing, instead is more inductive and emergent in its process. The goal of grounded theory and in-depth interviews in to establish “data categories and then examine relationships between categories” while discussing how research participants “lived or worked experience” can be understood. The quality of data, the scope of the research, the nature of the subject matter, the amount of useful and available information can be collected from each participant, the use of shadowed data, and the qualitative approach and analysis used are considered important factors in determining the sample size of a qualitative study. Instead of centered on “how many participants” can be wrong question and the rigor of the approach depends on the developing the set of applicable conceptual categories, the saturation of those categories, and the complete interpretation of the data (Dworkin, 2012).

According to Vasileiou, et al. (2018), the sample size determination can be guided based on the experts’ experience. In exploring a new and fresh topic, employing fewer individual interviews enabled researchers to manage the complexity of the analytics task. Saturation is the most important principles in determining the sample size of a qualitative study. Francis, et al. (2010) have suggested two key concepts on which the saturation is specified: (i) research should prior determine an initial sample of analysis to be used for the first round of analysis and (ii) a stopping criterion, which is, a number of interviews needed to be carried out further, the analysis of which would not yield any new themes or ideas. Applied in this study, nine practitioners from internal and IT audit field and RPA will be chosen as the initial sample size. The sampling continues until the researcher sense the saturation has accrued.

The sampling technique applied in this study is selective sampling. Selective sampling is a sampling technique whereby the qualitative researchers recruit participants who can provide in-depth and accurate information on the phenomenon of the research. It is highly subjective and defined by the qualitative researcher producing the qualifying requirements eligible for the participants (Statistics Solutions, 2015). The selected criteria for this study are: (i) practitioners in the field of internal or IT auditing; (ii) practitioners in the field of RPA; (iii) working experiences of more than 3 years; (iv) based in Malaysia.

3.3 Scope of Interview

Semi-structured interviews are used in a qualitative phase to explore new concepts to generate hypotheses. Semi-structured interviews are an effective method for data collection when the researcher wants to: collect qualitative, open-ended data; or to explore participant thoughts, feelings and beliefs about a particular topic. The purpose of this study is to understand the RPA implementation and the impact on the IAF. The purpose is developed in response to a subject matter that needs to be explored (Dejonckheere & Vaughn, 2019).

Semi-structured interview includes a short-list of ‘guiding’ questions that are supplemented by follow-up and probing questions that are dependent on the interviewee’s responses. Pre-defined questions are prepared during the interview, interviewee is encouraged to answer the questions freely and propose new questions (Jamshed, 2014). The interview will initiate with a simple, context-setting questions before moving to more challenging or in-depth questions. Interviewing is iterative in a qualitative study. Data collection and interpretation takes place simultaneously, which may lead to changes in the guiding questions as the study progresses. Questions that are not effective may immediately be replaced with other questions and additional probes can be inserted to explore new subjects raised by participants in previous interviews (Dejonckheere & Vaughn, 2019). As this study is conducted during the pandemic COVID-19, the physical meeting is not encouraged; thus, the data collection of this study is through online interviews via Zoom – a videoconferencing platform. The online interview also provided great flexibility for the interviewer and participants. Also, Zoom has the advantages of recording the interview session and storing it directly to ease data management.

This study is Malaysian based; therefore, the participants were selected based on selective sampling according to industry working experience and academic qualification. Participants will be approached through LinkedIn, and permission will be asked and obtained from each interviewee before carrying out the interview. This is to ensure that it took place at their willingness. An interview invitation that consists of confidential consent and interview questions will be sent before the interview session. The purpose, outline of the study, and some key questions will be sent to the interviewee for their preparation along with the invitation. In this study, four internal auditors, one IT auditor and four RPA developers were interviewed hence they became the samples.

3.4 Research Instrumentation

Describing the concepts used in qualitative research takes a more open-ended approach. During an interview, the questions the researcher decides will determine what data he ends up receiving from the participants. Unlike in quantitative research in which clear definitions must be explicitly spelled out in advance, qualitative research allows the concepts definition to emerge during data analysis (DeCarlo, 2018). The ideas in this study derive from the process of reasoning about what has been observed, using an inductive approach to conceptualization. In the course of the research, qualitative researchers inductively establish key concepts and continue to refine and evaluate the concepts through conceptualization and operationalization. **Conceptualization** is the process by which the researcher defines the concepts or constructs to be analyzed, and **operationalization** is the process whereby the researchers set indicators to measure the constructs (Brent D. Slife & Yanchar, 2016).

Throughout the interview session, open-ended questions were designed for the interviewees to answer the research question. The questioning process is limited to open-ended questions to the study's **constructs**: the key risk areas, changes in IA process and skillset required by the internal auditor. Each construct is divided into two **indicators**: implementation and technical, to measure the construct. The questions in each indicator set are designed based on the areas of expertise where the internal and IT auditors and RPA developers are involved in. In the other words, two set of interview questions are prepared given the different industry prospect where the questions of implementation indicator will be answered by internal and IT auditors, and RPA developers will answer the questions of technical indicator. The reasoning behind each interview question being prepared and asked will be discussed in Chapter 4.

3.4.1 Interview Questions

Constructs	**Indicators**		**Research Questions**	**Instrument**
	Implementation	**Technical**		
Key risk areas	What are the risks in auditing a bot?	What are the risks when designing an RPA?	What are the key risk areas within RPA implementation in an organization?	Open-ended question 1-5
	What is your recommended RPA risk management model?	What are the risks during the operational stage?		
		What are the risks after the implementation of an RPA?		
Internal audit process	Are there any needs of transformation of the internal audit process to audit RPA?	What are the differences of the RPA audit trail compared with other technologies?	What are the changes in the internal audit process for organization undertaking RPA?	Open-ended question 6-10
	What do you think are the differences in auditing the human work and auditing the robot work?	Do you think RPA would reduce the function of IA?		
	Do you think if RPA would reduce or increase the tasks of IA?			

Skillset	What are the skills required in auditing the bot?	Do you think the IAF is critical in assisting an RPA implementation?	What are the skillsets required by internal auditors?	Open-ended question 11-14
	What are the skills required in assisting RPA experts in implementing RPA?	What are the skills needed in monitoring the bots?		

3.5 Data Analysis

Ideally, qualitative data analysis takes place at the same time as data collection, so that researchers can generate an evolving understanding of research questions, which in turn informs both the sampling and the questions being asked. Eventually, this iterative data collection and analysis leads to a point in the collection of data where no new categories or theme arise. This is called saturation, which means that the collection of data is complete (DiCicco-Bloom & Crabtree, 2006).

In this research, the thematic approach (TA) will be applied as it is one of the most accessible qualitative analytic methods and it involves procedures that are common to most types of qualitative analysis. TA is used to evaluate most sort of qualitative data such as interviews, focus groups, and qualitative surveys. Researchers can capture dynamic, messy and conflicting relationship that prevail in the real world. TA enabled the researcher to recognise widely known trends and relationships to meaningfully address the research questions of the study (SAGE, 2019). According to Braun and Clarke (2013), TA involves seven steps: transcription, reading and familiarization, coding, searching for patterns, reviewing themes, defining and naming themes, and finalizing the analysis.

Transcription is when the researcher translating the recorded data into written documents. Transcription must be done to convert the spoken word to the written word to facilitate analysis. Once the transcription is complete, the researcher should **read** it and **familiarize** with the data, the transcript. In order to notice things of interest, it is necessary for the researcher to be familiar with the data (SAGE, 2019).

Coding refers to the identification within the entire dataset of all related pieces of data to answer to the research questions. Semantic code technique is applied in this study, as the research expects to present participants' experience in a more realist and descriptive way. Researcher starts coding the transcript and identifies the semantic codes, the code can be labelled with a name that is derived from the data itself. The three research questions will be developed to capture the data (SAGE, 2019).

Once the coding of the entire data set is complete, it is then the searching for **patterns** within the data. Pattern-based analysis enable the researcher to recognise salient data characteristics that are vital in addressing the research questions. The frequency of the codes appears need to be considering carefully as certain codes that able support the answer to the research question may do not appear often. Then, the researcher needs to identify the broader patterns of the data that can be identified as **themes** and sub-themes in order to answer the research question. Theme is also known as a central organizing concept, a set of codes, which is a series of ideas or aspects that can be documented under a particular theme. The themes and sub-themes need to be properly **defined** and rename in order to better structure the results and answer (SAGE, 2019).

Lastly is the developing of the **analysis**. This is usually where the thoughts of the participants can be distilled, summarized and told in a way that is both respectful to those participants and relevant to readers. There are a variety of ways in which researchers can synthesise and present their findings, but direct quotes from the participants must support any conclusions drawn by the researchers (Austion & Sutton, 2015). At this final stage, the development of themes and sub-themes could answer to the research questions.

3.6 Ethical Consideration

This study takes responsibilities to comply with the ethical principles to protect the interest of the participants in order to ensure the data security. The matter of ethical research is the basis of this study, the researcher should ensure that participants are safe from harm and are protected from unnecessary stress. In order to avoid unwanted research dilemmas, it is therefore important to ensure that careful planning and ethical standards are adhered to (Cacciattolo, 2015).

Due to the study process's in-depth nature, ethical issues have particular prominence in qualitative research. Interview-research abounds with ethical issues. There are a few aspects to consider when conducting an online interview study. Some are connected to the risk that the interview participant will unwillingly reveal more than was intended because online identities or environments contain details not specified in the consent agreement (Salmons, 2012). Informed consent is a process for ensuring that people understand what it means to engage in a research study to determine whether or not they want to participate in an aware, deliberate manner. Interviews allowed researchers to meet with other people, and consent should be aware to the participant. In this study, an interview invitation (see Appendix) is prepared and send to potential participants that includes ethical consent such as the purpose of the research, the fact that participation is voluntary and that one can withdraw at any time, how confidentiality will be protected, the contact information of the researcher (Mack, et al., 2005).

As qualitative research is conversational, it is imperative to maintain data confidentiality. The researcher utilised Zoom because the software was able to secure the record and store sessions without recourse to third-party software. This feature is essential to protect the collected data. In addition, the transcript of the interview will not be shared with anyone except when requested by the interviewees.

4 Results, Findings and Discussion

This chapter allocated importance to data presentation and analysis based on the data collected. The results are presented and analysed based on the transcript information collected during the one-to-one semi-structured interview sessions with two groups of participants: audit practitioners and RPA developers.

Two sets of interview questions were designed based on both the implementation and technical indicators are prepared. Responses from both sets of interview questions were integrated to answer the research questions. Four internal auditors and one IT auditor have answered the **implementation indicators' questions** *(see Interview Question I-1 to I-7)* throughout the interview, and four RPA developers have answered the **technical indicators' questions** *(see Interview Question T-1 to T-7)*. In this chapter, the participants' responses to the semi-structured questions asked in the interviews are recorded. The data collected from the interview are presented in the transcript form, and it is analysed by carrying out contextual coding analysis. The following section is structured as follow: the first section outlined the profiling of participants; the second section laid out the responses from both implementation and technical interview questions that were to direct the research questions, and the third section presented the contextual coding analysis based on the responses from both indicators.

. 4.1 Respondents Profiling

The respondent of implementation indicators comprised of one chief financial officer and one group internal auditor with more than 20 years of experiences in the field of auditing, one internal audit manager with 10 to 15 years of experiences, one internal auditor and one IT auditor where both of them have 3 to 6 years of working experiences in the field of internal auditing.

The respondent of technical indicators questions were four technology enablers that major in RPA development, where most participants have at least 10 to 15 years of working experience. While one has 3 to 6 years of working experience in enabling RPA solution. As this study is Malaysia-based, all the participants are either Malaysian or have worked and based in Malaysia for at least 3 years.

	Professional Qualification	**Years of working experience**	**Current designation**
Respondent number code for implementation indicator			
R1	ACCA, FCCA	15 years and above	Chief Financial Officer
R2	Master’s degree, CIA	15 years and above	Group Internal Auditor
R3	Bachelor’s degree	3 to 6 years	IT auditor
R4	Bachelor’s degree, ACCA	3 to 6 years	Internal auditor
R5	Bachelor’s degree, CIA	10 to 15 years	Internal audit manager
Respondent number code for technical indicator			
R6	Bachelor’s degree	10 to 15 years	Technology enabler
R7	Master’s degree	3 to 6 years	Financial system specialist
R8	Bachelor’s degree	10 to 15 years	RPA developers
R9	Bachelor’s degree	10 to 15 years	Automation analytics

4.5 Data Findings

This session allocates importance to data findings based on the data collected. In this session, the researcher will discuss the key themes that arose from the contextual analysis and then merged the discussion from implementation and technical indicators to answer the research questions, satisfy research objectives, and solve the research problem. In this context, the participants who answered the implementation questions (internal and IT auditor) are collectively referred to as “implementation interviewees,” and the participants who answered the technical questions (RPA developers) are collectively referred to as “technical interviewees.”

4.5.1 **RQ1**: Key Risk Areas Within RPA Implementation

In terms of **implementation indicators**, from the contextual coding analysis, four out of five interviewees mentioned some **risks around the robot**. One of the interviewees highlighted that *“Intervention of the environment surrounding before you reached the bot, is what you would need to audit [...]”* (R1). The interviewee further mentioned that the system users, the developers, instruction to the bot and right of access to be the risks around the robot. Amongst the risks, three of them highlighted the risks of the **right of access**. R1 described *“[...] who can change an item in the bot and who has access to the bot”* while R4 hold that *“the first risk will be the access over right (of the human)”*. To applications, a bot is just another user that needs to authenticate to use most systems. To secure a bot, access control for humans and bots are equally critical (Tolly, 2019). Another interviewee (R3) illustrates that *“There are some other risks including [...] and the privilege of bot access”*. RPA software bots require privileged access to perform.

Data protection is also amongst the major risk that needs to be considered. RPA implementation comes with several risks and internal privileged access right that have the potential to be exploited. This can lead to the confidentiality, integrity and reliability of data that organization processes being compromised (Capgemini, 2019). One of the interviewees (R4) mentioned cybersecurity risks such as hackers and ransomware, and other interviewees highlighted the data of integrity such as *"[…] whether the bot changed out the integrity of data"* (R3) and *"[…] data integrity […] we need to understand how the bot generates and maintains the data"* (R5).

Technical risks are also identified during the contextual coding analysis. The developer's capabilities and instruction to the bot were also appeared to be the key consideration when auditing a bot. R1 presented *"Auditors would need to audit […] who instruct what the bot does […]"* and R2 illustrated *"[…] whether the programme is set correctly […] whether the person who does the programme construct it properly"* and *"[…] whether the person who handles the robot has the right and enough training to control it"*.

Most interviewees have also found that **auditor's capabilities** to be the main risks in auditing a bot. One of the interviewees (R1) expressed that the current auditor had not been trained adequately to tackle the risks of new technologies. It is consistent with R2, who agreed that the most significant risk is the auditor skills and capabilities to audit an evolving technology. Interviewees suggested that auditors must understand the technology such as *"[…] understand what does this bot do, what does this bot track"* (R3), *"it is crucial for auditors to understand the RPA"* (R5) and *"[…] about the training and understanding the robot's limitations"* (R2). This risk corresponds to RQ3 of this study, which aims to examine what are the skillset required by the internal auditors.

From the interviews, the implementation interviewees hold the same opinion that **any technology-related risk framework can be adapted to an RPA risk management model**. The risk management model includes managing risks faced by the organization as a whole and the individuals involved with all operational processes. Generally, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (COSO-ERM) framework and the framework of the International Organization of Standards (ISO) 31000 series are widely recognized for organization-wide risk management (Horvath, 2020). *"IT-related risk management models are similar […] risk management proposing for RPA is the same risk management model they apply for all technology related,"* (R1), *"I believed is COBIT framework because it is related to IT,"* (R3) and *"the model is relatively standardized […]"* (R4). R4 further explained that it is challenging to tackle the risks of the robot with a proper framework taken the three ERM, COSO and IIA framework together in Malaysia conglomerates companies, as there is less Malaysian company practices ERM or COSO framework and IIA in the Malaysia market is still under-recognition. R1 also justified that an IT-related risk management model generally breaks it into three parts: *"before you get on the robotics process, while you get on the process and after you get on the process […] before you do something, you must make sure it is correct, while you do something, you must make sure it is right, after you do something, you must make sure all the loophole is covered."* It is also corresponded to the designed technical interview questions that aimed to understand the risks of each phrase of RPA implementation.

Lastly, one of the interviewees (R4) mentioned the **cost of implementing RPA** in Malaysian conglomerate organizations. *"It would take quite some training hours for employees to get used to the new systems […] the system might be costly at the moment […] how is the management going to recover the ROI […]"*. The most common tool to measure the ROI of an RPA is the Full-Time Equivalent (FTE) calculations (Digital Workforce, 2020).

In terms of **technical indicators**, from the contextual coding analysis**,** unstructured process, nature of the bot, change management and operational and execution risks appeared to be the main risks within RPA implementation. All technical interviewees highlighted that the **unstandardized process** would cause the failure of an RPA during the design phase. Deploying robots to run the process is challenging if there is no standard process to follow. It is crucial to understand the maturity of the processes and decide which processes are standardized enough to benefit from RPA and which processes would benefit from harmonization and standardization before starting an RPA initiative. (Celonis, 2017). Interviewees expressed that *"unstandardized process causing the failure of an RPA,"* (R7), *"we need to discuss with operational team to standardize the process, for example, collect the data only from one resource or one system […]"* (R8), *"we need to ensure the process that we wanted to automate is fully structured and mature enough,"* (R9). R9 further provided an example of a non-standardized process, *"requires human decision-making, it cannot be automated; unless the decision has a specific direction that can be followed […] process need to be lean enough to be automated."* An RPA developer (or an RPA analyst) determine the level of process standardization by mapping and visualize the components of the processes. They collect details of the process end-to-end and determine the input, output, steps, used files and folders, website and platform of the process. If there is any lack of components collected, it will also cause the failure of an RPA. For example, R7 highlighted that the lack of input data would disable them to design the RPA correctly and use them effectively.

In addition, R8 also mentioned the risks of **unstandardized data**. RPA required structured data, but 80% of enterprise data is buried in unstructured documents (Pritzker, 2020). *"Data collected from different systems and locations would increase the process complexity."* Process standardization should be done to be applied in multiple sections of the organization; if it is not, the developer or analyst will reconstruct and simplify the process, which is called **process improvement**. Six Sigma and Lean methodology can be applied to optimize and standardize the process (Fernando, 2020). *"We will try to simplify the process as lean as possible […] it needs to be improved before we can automate the process. It can take one or two years for the team to improvise their process."* (R9). From here, it also can be seen that RPA has become a catalyst in promoting process improvement by identifying the process standardization and opportunity for automation.

Companies often underestimate the degree of change that comes with implementing a new IT system. **Change management risks** have also inducted from the responses of technical interviewees. RPA implementation requires considerable effort to manage the changes brought to the process and job contents of employees. Mismanaged change management across the organization can cause the failure of the automation efforts (Priyadarshi, 2019). R6 illustrates that the lack of users' support and unclear expectations on RPA will result in risk when designing an RPA, *"Lack of training for business users will results in them not knowing how to use the RPA […] results in underutilization of the robot"*. Also, the business users for RPA are usually non-technical personnel, and if they are not trained in applying best practices, it can also lead to a security incident. At the same time, R7 agreed that business users must recognize the benefits of automation. Besides, R7 highlighted a fact where the process of dealing with stakeholder is essential: *"[…] they need to deal with the stakeholder, can they change this? Can they change that? […] a lot of agreements need to be in place."*

Data security also among the top concern for technical interviewee -- *"we have to ensure all the security and compliance are adhered to (when designing and developing a bot)"* (R6). R6 further highlighted the risks if a bot and the developer need to deal with sensitive data; a non-disclosure agreement (NDA) must be in place when developing an RPA. There will be a risk of breaching company compliance when the developer does not correctly do bot testing. R6 also declared that *"their individual ID should only be accessible to a specific part […] we are not supposed to get anything more than the particular parts to script the use case."* Another two technical interviewees mentioned **bot credential**, where interviewee R7 explained the bot credential issues. He claimed that *"when RPA replaces the human to perform the tasks, RPA will have their own ID to login into their own system."* RPA operate at the presentation layer and constantly access different applications to operate. If the credentials leveraged by both RPA admins and this new digital workforce are left unsecured, an attacker can steal them and gain access to the system and data. R9 also raised concerns: *"if the users wanted to log in this page […] do they need to have a login password?"*.

One technical interviewee (R6) specified that developer usually follows an **RPA development standard** to script the particular RPA concept during the design phase. UiPath Robotic Enterprise Framework (REFramework) are one of the most recognized development frameworks that R6 is using when developing RPA. The framework is meant to be a template that helps the developer design processes that offer a way to store, read, and easily modify project configuration data, a robust exception handling scheme and event logging for all exceptions and relevant transaction information. The REFramework ensures the code quality and is useful for continuous code quality (UiPath, 2020b).

Other than that, two technical interviewees acknowledged that the **change request** from users is the risk when developing and after implementing an RPA. For example, R7 stated that *"the main risk would be after we implement (the RPA), the flow of the process would need to change due to some unexpectable reason […]it will result in the RPA that implemented is not able to use […] there will be a new system"* and R9 highlighted *"after the bot goes live, the risk can be the change requests from the user […] we need to re-do the analysis and re-design the flow […]"*.

When developing the bot, they also look at the **nature of the bot,** such as the RPA compatibility with other systems and system exception. *"System exception is the behaviour of the system, since RPA is dealing a lot with other systems, we need to look in-depth other system's behaviours as well […] is there any security breaching with that system, or are there other users who are not part of the company using the system?"* (R6) and *"when designing the RPA solution, we need to think about the compatibility of RPA […] In a company of using SAP ERP […] our design should be reasonable, even for other processes and systems."* (R8)

One technical interviewee (R8) illustrated the **cost of implementing RPA**. *"One of the risks I can see from a business perspective is the FTE calculation […] if a human being is doing these many transactions manually in six hours, we need to examine how the robot will do it and the cost we save […] we need to consider the license cost for the RPA also […] the risks while selecting the appropriate RPA tool, based on the cost and license."* According to Moayed (2018), there are four major categories to consider on the cost side: the cost of automation tool (license cost), the extra cost of infrastructure, the cost of development and the cost of monitoring and maintenance.

One technical interviewee (R6) brought up the **technical risks** such as failure of coding and schedule testing. *"It was not coded or appropriately programmed […] supposed your robot is to run for one hour, but the testing is not being done correctly […]."* The failure of appropriate code the bot and testing of the bot would result in data security risks as well as **operation and executive risks**. All technical interviewees have considered operation and executive risks, and it is mainly occurring after the implementation of an RPA. For example, R6 mentioned *"the risks are when the bot does not execute how it is supposed to be completed due to environmental, network, or infrastructure issues […] if the business operations cannot continue with the particular process, and we will have significant downtime […] (failure in schedule testing) results in the robot cannot complete specific tasks that are remaining in the emails or the shared folder, there will be incomplete tasks […] it will also breaching of compliance if the bot testing is not being done properly."* R7 also agreed that *"when robot system suddenly down, for those processes required to perform within the turnover time, there will be some issues […]"*. R8 and R9 highlighted when bots stop working due to coding failure or the applications that have been automated are not working. It may cost damage to the organization as the data may become chaotic.

The malfunction of the bot subsequently required the **intervention of human**. The intervention of human was categories into two part: business exception and back-up of human workers. R6 and R9 declared that the business exception needs to be identified during the design phase of a bot. The business exception is also called "rules-based rejection" and any exceptions to the automated process need to be assigned for the human to manage (Singh, 2019). Then, *"if the RPA system down and the tasks cannot be done on time, which will eventually need humans to perform manually [...] humans might not be able to catch up to perform the tasks within the timeline,"* (R7), *"we need people to go for manually complete the transactions [...] but nobody knows or familiar on how to do the processes [...]."* (R8)

4.5.2 **RQ2**: Changes in the Internal Audit Processes

In terms of **implementation indicators**, from the contextual coding analysis, six areas of changes in the internal audit process are identified: three inputs (internal auditor knowledge and skills, audit tools, time and efforts), audit techniques, internal audit practices and challenges in auditing. **The Knowledge and skills of internal auditor** are highly concerned by most interviewees. For example, *"the internal auditor needs to understand the basic technological knowledge, how the robotic programme is structured [...] the robot's installation, how the training is being conducted to business users [...] chief internal auditor needs to evaluate the robotic automation function"* (R2), *"auditor need to look at the process on how the system works"* (R5). In an IT-comprehensive business environment, most interviewees highlight the need of IT audit skills, *"to audit RPA, the auditor needs to understand more IT details [...] the number of IT auditor might be significantly increased in a team"* (R4), *"there will be an emergence of requirement on somebody who can do both finance and technology"* (R1), *"IT audit is highly demanded [...]"* (R5). This input factors also correspond to the third research question of this study – the skillset required by the internal auditors.

The second changes will be in the use of **audit tools and techniques**. Three interviewees noticed that the use of audit tools might change when auditing in an RPA environment. For example, R4 pointed out that software and system to check on the company process validation is crucial when RPA is deployed in an organization. R5 agreed that *"for the data integrity issues, we required many IT auditing tools, to look into the data and information generated by the robots."* R5 further specified that some audit analysis tools such as CAATs can be adopted to do the preliminary analysis on the data and information extracted from the system. While R1 brought up the fact that since the robot process a multitude of information, data mining needs to be conducted to crone and make sense out of the data.

The input of time and effort by the internal auditor has also been determined by the implementation interviewees. They agreed that time and effort has greatly reduced if RPA is deployed in an organization, as *"a robot will be very straightforward and only one answer will be given [...] much easier when compared to auditing human work [...] I assume we can reduce the manpower up to 10 people for the internal audit team [...] robot work is easy to be verified"* (R3), *"the robot work does not have many mistakes [...] human tend to have mistaken, lousy handwriting and slow processing time [...] reduced our time for reviewing the document"* (R4), *"auditors might not need to have communicated with humans, such as asking documents and posting questions [...] we just need to rely on the data"* (R5). R5 also pointed out that RPA can significantly reduce the travel and transportation time, *"as we do not have to go to the auditee site [...] if the auditing system can synchronize with the automated system used [...] data can be easy extracted."* R5 put forward an idea of synchronizing the auditing application and the automated system, and it could be explored in future studies.

Three interviewees raised the changes in the **internal audit practices** from two perspectives: changes in audit target and focused on the data. In terms of audit target, instead of auditing human work, *"the auditor would need to audit the person who programs the robot to ensure that the detail is concerned [...] auditor would need to audit the exception report, the right of access"* (R1), and *“we need to know how the management instructs the developers to do the programming and also how they trained the company staff on how to use to programme, how to overcome problems with the robots, how to do the maintenance […]”* (R2). Also, one of the implementation interviewees (R5) pointed out that. *“auditors now only need to focus on the data generated by the robot”*. Given the changes in internal audit practices, there is also some concerns raised by the interviewees regarding the **challenges in auditing the bot**. R2 and R3 indicated that the nature of the bot – no judgmental involves could be challenging to the internal auditor if the auditor did not know how to control the bot. R1 are the only one proposed that RPA will increase the tasks of internal audit, she mentioned that *“the increase will be in terms of rechallenging the process that they previously knew it”*. While R5 illustrated that *“back to the data, auditors need to ensure the completeness and (only they can) rely on the data”*.

In terms of **technical indicators**, two questions were asked to technical interviewees to pertain their view regarding the changes in the internal audit process from a technical perspective. Four themes are identified: changes of audit target, the way of collecting evidence, the importance of documentation and the reduced internal audit workload. In terms of **changing of audit target**, R7 view the implementation of RPA shift focus from doing audit the process being performed by the human to audit the process performed by the robot, the target audience changed from human to robot, while R8 advises the auditor to assess the integration of RPA with other systems.

R6 stressed the **importance of documentation**. The interviewee possessed that the process documentation is crucial for the internal auditor to understand what the bot does. It is important for the users to update the documentation as well. *“The main area of an RPA audit is basically they need to look at the documentation versus business processes […] business team is responsible for updating the certain documentation […]”* (R6).

All technical interviewees proposed various ways for the internal auditor to **collect audit evidence** when auditing the RPA system. R6 presented that the design of an RPA bot that could assist the internal auditor: *“the developer can design the RPA robot to produce a certain level of reports that would be useful for the internal audit function […] such as status update report”* (R6). R7 and R9 highlighted the benefits of RPA for internal audit, which *“inside RPA system, it will have a proper record of the step-by-step, including the screenshots on how the process been performed […] like Excel, it would not have the list of steps taken to come out with the final report, but for the RPA, they will have these steps.”* (R7) and *“in RPA, every action taken will have a log […] if the bot crash in between, we can open the log and see until when and at what point the bot has crashed […] auditor can directly audit the data executive by RPA*” (R9).

Although half of the technical interviewees asserted that the RPA would reduce the function of internal audit, while half against; all technical interviewees supported that RPA could **reduce the internal audit workload** by making the audit tasks more manageable to be done. With the status update report, audit logs, proper step record, they agreed up to a certain extent, RPA eases internal audit work. R8 explained her view in detail, where *“the bot is implemented with standard code […] release many numbers of errors […] definitely helps to reduce the activities for the internal audit because we have already given the logic for the bot to do the work.”*

4.5.3 **RQ3**: Skillset Required by Internal Auditors

In terms of **implementation indicators**, from the contextual coding analysis, five main themes are recognized: technology knowledge, IT audit skills, business process knowledge, communication skills and competitive personalities. Two interviewees highlighted the auditors must need to equip with **knowledge of technology** existing in the organization for better audit them. For example, R2 stressed that *“the internal auditors need to be equipped with the knowledge about the* *current technology and understand what the program is being used […].”* He further explained the importance of this factor to achieve the ultimate audit objective – *“ensure that the robot functions as required, ensure the maintenance is done, ensure the support is available whenever there is a problem.”* Also, R4 highlighted the demand for data analytics skills for internal auditors to audit the bot. It also corresponds to internal audit practices changes where internal auditors need to utilize data analytics to audit the bot's data and information processes.

Most implementation interviewees pointed out the **IT audit skills**. R3 illustrated that *“basically whatever skills IT auditor have right now, they can audit the bot […] they need to brush up a few of their skills […] and update it.”* R4 also brought up the importance of the security system. He further recommended that the internal auditor to understand the system’s security features to ensure that the bots are running accurately and without compromising security threats. While R5 put IT audit skills as the most important skills in auditing a bot, specifically, they need to equip themselves with the IT auditing tools, as he mentioned *“the demand for IT auditor is very high because of the changing of the current landscape and the pandemic […] the IAF needs to be established with these IT tools.”*

Most implementation interviewees specified the **business process knowledge**. R1 highlighted that in an RPA environment, a person who is very detailed in processes is highly needed. R3 and R5 agreed that internal auditor must have in-depth knowledge of business processes and subject matters on process improvement. While R4 supported that internal auditor is critical in assisting an RPA implementation, *“as they have been the “checker” of the conventional processes.”*

In assisting an RPA implementation, one interviewee (R3) suggested that the person must have strong **communication skills**. *“He must be able to understand the requirements of the stakeholders and translate it very well*.” He further explained that the requirement stage in reviewing a project is very critical. The interviewee also agreed that the internal auditor needs to work together with an RPA developer, *“as in the past, if a company want to implement an ERP, the internal auditor also works together with a software engineer to make sure exception handling.”*

Lastly, some **competitive personalities** also identified based on the contextual coding analysis. R1 stressed the importance of fast-learning and applied logic, *“the internal auditor must have personalities and ability to learn a new threat very fast […] and able to process logically and asks logical questions”*. She also suggested skills of troubleshooting is still lacking in the current market; therefore internal auditor could workings on it -- the ability of *“troubleshoot what has gone wrong and tell a consultant and engineer on what to amend.”* It is also agreed by R2 who illustrates the importance of internal auditor to detect any wrongdoings within a bot.

In terms of **technical indicators**, from the contextual coding analysis, four main themes have been identified. All technical interviewees agreed that the IAF is critical in assisting an RPA implementation considering their knowledge and subject matter in accounting and auditing, and in business process. Most interviewees recognized the importance of internal auditor, in specific their **knowledge in accounting and auditing**. R6 mentioned that *“internal audit will be an additional check in terms of functionality and automation of the particular process to ensure that the programme is accurately to carry out this business process.”* R7 also agreed that the internal auditor is critical in implementing the controls in RPA documentation and process. It is also complemented by R9, *“from the business wise, how to know that our automation for accounting system is okay or not? For sure we need to be audited.”*

In terms of **business process knowledge**, R8 hold that, at the first place, as internal auditors are subject matter expert in business process, they are critical in standardizing the process before an RPA came in. The business process knowledge also highly valued by all technical interviewees in monitoring the bots. R6 mentioned that the monitoring process is usually done by a business process specialist, the monitoring effort required understanding the business process itself. R7 illustrated *that "when you are monitoring the bots, you would need to understand the business process […] you need to assign which process to go first […] on which steps are more critical to be performed first."* R8 hold a similar opinion, *"they need to know the models created for the business process and how it has been split into this section while developing."* It is also agreed by R9, *"you need to know what the (process) inputs and output are, and whether the bot works properly."*

Most technical interviewees interpreted that **technical skill** is significant in monitoring the bot. The interviewees clarified that monitoring the bot does not require extensive programming skills; but the technical skill to understand the system and the technology. R7 appended that, *"internal auditor needs to have certain knowledge on maintaining all the password for the robot, and the system that they (bot) want to perform the tasks […] there will be some challenging for internal auditor as they need to catch up the new system to understand it."* One interviewee (R8) advised that, *"internal auditor should know on which platform the bot has been built […] aware of the agile methodology and software development lifecycle […] how the bot has been developed, get all the details from the developer."*

Lastly, in terms of the importance of internal audit, two interviewees opined that **quality management system** should be performed. *"RPA will work with continuous improvement leads such as Six Sigma, blackbelt […] the support person should have documented every time the problem happens […] keep documenting those to help improve the bot."* (R8) From the technology-wise, R9 elucidated that internal audit is critical in assisting the organization in attaining ISO certification by ensuring the systems are up to standards.

4.6 Relating Findings to Research Questions and Objectives

This section extends to interpreting the findings merged from the discussion of implementation and technical indicators, linking it to answer the research questions, meeting research objectives, and eventually solving the research problem. As this study is internal audit-based, the implementation discussion is mainly discussed to answer the research questions, while technical discussion will be used as supported arguments. The following topics (findings) are originated from the interviewees' responses, and each topic is referenced to the relevant literature review to substantiate the points being made during the interviews.

4.6.1 Research Question 1

Objective 1: To explore the key risk area within Robotic Process Automation implementation in an organization.

Question 1: What are the key risk areas within Robotic Process Automation implementation in an organization?

The first objective relates to addressing the first impact of implementing RPA on the IAF that is specifically its "key risk area" brought to an organization. The objective is built to investigate the new risks and control considerations that need to be considered by internal auditor when an organization deployed RPA. The findings are qualitatively answered by two groups of interviewees who responded towards the research question and objective from two perspective: implementation and technical. The interview questions for this objective were carved differently but discreetly embedded the strength to meet the research question and objective. In terms of RPA deployment, auditor need to understand the **risks around the robot**. From the discussion analysis, a total of **nine key risk areas** were identified.

Risk 1: Right of access

In RPA, there is two dimensions of right of access: access of bot and access of human. In a process automation where thousands of software robots are deployed to perform tasks, each one of these bots required privileges to connect to target systems and applications to perform assigned duties. If these non-human credentials are left unsecured, they may become prime targets, violating data security and privacy. This means an RPA implementation must has a solid privileged **credentials management and security strategy** (Turner, 2019). To be trackable and auditable for monitoring, a bot needs to be identifiable. The RPA robots identify needs to be properly stored in a source of record (Schuett, 2019). For example, in Blue Prism, there is a centralized source of record for all robots from all RPA products within an organization, it is called as "Control Room". In terms of access of human, people still need to work with bots to plan, run, view and edit their processes, in an attended automation. There are some threats of human workers exploiting the bot's privilege access to steal and manipulate business-sensitive information. Thus, role-based access control (RBAC) is encouraged to build into a RPA system and allows companies to limit access to only approved users while segregating automation-related tasks between employees (Electroneek, 2020b).

Risk 2: Data protection and security

An RPA preserves an organization's data integrity to a certain extent by minimizing human error and ensuring that data is continuously synched and updated. However, any vulnerability could result in a danger that expose sensitive data and puts the organization at risk of data theft. Roy (2020) proposed that the organization can implement few steps to ensure the RPA data protection: multi-layer authentication, encryption and access control. When business process involving the processing of sensitive data are automated, the scalability of RPA should be considered. In certain cases, a violation of confidentiality may have a serious effect on the company thus, an additional control should be incorporated into the workflow to minimize the risks (Pluzhnikov, 2021).

Risk 3: Technical risks

Technical risks are the failure of developers' capabilities to properly instruct a bot. Poor design, operational bugs, or inadequate security measures are the inherent technical issues underlying every software. In RPA, these issues will result in unplanned downtime, which will have an effect on the workflow (Joshi, 2019). The developers may face various technical risks due to the unstandardized process and data that needed to be automated. Some of the technical interviewees also highlighted the changes requirements for an RPA project will caused to the technical risks. As a consequence, careful attention to detail when developing an RPA is important. Scope creep is to be anticipated during the implementation phase, as the iterative back-and-forth between the developers and business teams will certainty yield new insights into process and logic details that necessitate configuration changes. Once the robot is up and running, risk mitigation requirements include continuous oversight of inputs, outputs and process. An RPA project can also be disrupted by a lack of adequately automation specialists and process subject matter experts (ISG, 2020).

Risk 4: Auditors' capabilities

The audit team faces difficulties in terms of existing skills due to the rapidly evolving market climate. The rapid development of business, combined with the increasing complexity of financial reporting requirements and the opportunities or risks posed by technological advances, necessitates greater specialisation within the audit team (Barac, et al., 2016). As a result, it correlates to the third research construct of this study, namely skillset required by the internal auditors. This topic **of skillset required by the internal auditor** is discussed in the Section 4.6.3.

Risk 5: Change management risks

RPA implementation is distinct in that it is not usually used by an organization's IT department. Instead, those who are directly involved in the process that is being automated, are the ones who operates RPA, the process owners (Kokina & Blanchette, 2019). RPA's business users are generally non-technical personnel, and poor change management will lead to RPA failure. EY (2017) recommended businesses that are adopting RPA to develop a **business-led RPA CoE** to manage and improve the virtual workforce. Furthermore, there is a risk where the organization invested substantial automation resources at a high cost but with only little additional benefits, due to the failure to adjust internal processes to allow RPA to operate through as much of a process as possible, resulting in reduced savings. As a result, the CoE processes must be in place, IT governance must be decided upon, and workers must be trained to operate robots.

Risk 6: Nature of the bot

This risk is primarily related to changes in other system changes that underlying automated process and the compatibility of the RPA. Bots are trained to communicate with a small range of applications or browsers will become dependent on any changes to the underlying systems. If the IT department needs to deploy an update, vital patch, or some other enhancement, they must be aware of how the system change will affect the bots that communicate with it (DeBrush, 2017). System exception also needs to be considered. System exceptions apply to system-based incidents such as non-responsive systems, programme failure, or any modifications to the application that were not accounted for or recorded during the RPA design and implementation phases. If an exception is left unhandled in an unattended automation, it can significantly restrict RPA functionality. Since RPA works at the application's presenting layer, the company must ensure that the RPA tool is compatible with the applications that will be used to automate processes. In the other words, the company must choose RPA software that easily integrates with a wide range of software and platforms (Joshi, 2019).

Risk 7: Operation and executive risks

Operation and executive risks arise when bots do not operate as planned. This can be triggered by technical risks, nature of the bot, change management risks, and exception handling. Breaking bots have been one of the most concerning issues for an effective RPA implementation; the problem of breaking bots is also prevalent, preventing the organization from scaling. Modern business applications are highly complex, despite the fact that bots are highly organized. New features, bug fixes, changing dependencies, and design updates can cause an obedient bot to malfunction. It ultimately resulted in a high cost of maintenance (Walter, 2019). When the bot is not functioning, it required business users to manually perform the tasks if the tasks need to be done within required schedule.

Risk 8: Intervention of human

Other than system exception, there is also **business exception handling** in the bot context. The business exception is when a bot is unable to process a transaction due to its programmed instructions. Interventions of human often involve in business exception handling. To prevent incomplete tasks, it is recommended that bots in an unattended RPA be configured to alert human supervisors (in form of E-mails) immediately about incomplete transactions due to the business exceptions. Furthermore, the implementation of RPA introduces new positions in an organization for efficiently assessing bot performance (Joshi, 2019). They must "intervene" with the bot in order to reconfigure the RPA programme, and they must function as backups if the bots are malfunction.

Risk 9: ROI of RPA

From the business perspective, the management need to consider **cost of implementing RPA**. According to one of the implementation interviewees, a chief internal auditor often involving in evaluating the returns of investment of an RPA project. To fully realize value from implementing RPA, the company must invest in the capability to drive automation. This involves re-engineering process and navigating various stakeholders and business units. Some studies reveal that when management expects value to be derived without investment, capital or stakeholder alignment, the RPA project's ROI can be reduced (Bendor-Samuel, 2018). It is also agreed by EY (2019), where they revealed that one of the biggest reasons RPA projects fail is the level of RPA maintenance and support needed for in-production bots. It is because constant break-fix cycles that push bots out of production result in high maintenance costs, preventing them from delivery the anticipated ROI (Blue Print, 2020).

It is important for organization to have a proper risk assessment for RPA using a **standardized risk management framework**. The business environment becomes vulnerable to risks whenever a new technology, such as RPA, is implemented. It must be followed up with a programme of maintenance and control. A rigid governance framework must be designed for tracking, updating and minimizing any foreseen and unforeseen risks. According to the implementation discussion, interviewees agreed that any technology-related risk management framework can be adapted to tackle the risks of RPA. There are also a few ready-made RPA risk management framework introduced by Big4 and international institutions that can be adopted by the IAF to tackle the RPA risk and conduct a risk assessment. A robust risk management framework should include **identification, evaluation and assessment, prevention, reporting and monitoring, and governance** (Petters, 2021). As the research objective 1 is solely aimed to explores the key risk areas within an RPA implementation, it is notable that the proposed framework of Figure 6 could be adapted to an RPA risk management framework in terms of risks identification.

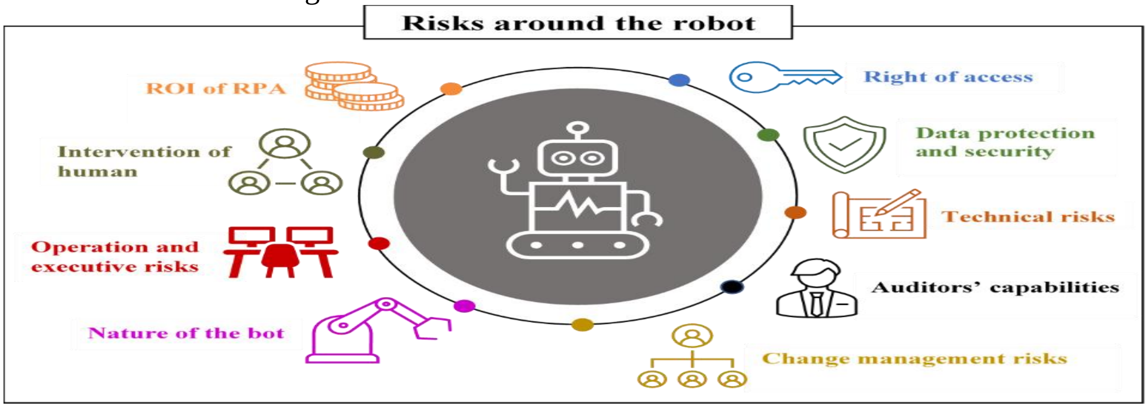


Figure 6: Proposed Framework for Key Risk Areas Within the RPA Implementation (Risk Identification)

4.6.2 Research Question 2

Objective 2: To understand the changes in the internal audit process for organizations undertaking Robotic Process Automation.

Question 2: What are the changes in the internal audit process for organizations undertaking Robotic Process Automation?

The second objective relates to addressing the second impact of implementing RPA on the "changes in the internal audit process" of an IAF within an organization deploying RPA. The objective is built to identify changes in the internal audit process when an RPA is deployed in an organization. The findings are qualitatively answered by two groups of interviewees who responded towards the research question and objective via from two perspective: implementation and technical. The interview questions for this objective were carved differently but discreetly embedded the strength to meet the research question and objective.

<u>Changes 1: Input of internal auditors' skill and knowledge</u>

The first impact on the internal audit process will be the input of internal auditors' skill and knowledge. IPPF Code of Ethics Rule 4.3 regulates internal auditors to work on improving their proficiency in delivery quality services (IIA, 2019). In determining a quality audit service, the International Auditing and Assurance Standard Board (IAASB, 2014) also urged auditor to be equipped with sufficiently knowledge, skill and experience. Auditors need to understand the technology deployed in an organization only they are capable in auditing them. Thus, the sufficient and appropriate skill and knowledge is crucial for internal auditor in auditing an RPA environment. The skillset required by the internal auditor is further discussed in Section 4.6.3.

Changes 2: Input of audit tools and techniques

In general, audit tools and techniques referred to any instruments auditors used in assisting their fieldwork, such as risk-based audit planning, quality assessment review tools and benchmarking, flowchart software, data mining, continuous auditing, electronic workpapers, Computer-assisted Audit Tools and Techniques (CAATTs), balance scorecard, process modelling software, statistical sampling, control self-assessment, etc (Bailey, 2010). The use of audit tools and techniques is important and useful during an audit engagement in gathering of reliable audit results (Motubatse, et al., 2015). In an RPA environment, as robot is replacing the traditional ways of operating daily activities, adoption of emerging audit tools and techniques or CAATTs must be considered by the internal auditors. For example, the use of data analytics and data mining can be employed to access the robot-generated data to test the data integrity.

Changes 3: Input of auditors' time and effort

Often, audits took longer than the time allocated due to the inefficiency in the audit process such as the failure of time management and unexpected problem during audit evidence gathering (IIA, 2020). RPA reduced the internal audit time and effort as it is easily accessible and straightforward. In realising the synchronization of the robot-generated data with the audit software or implementing a Cloud-based-RPA, internal auditors are then not required to go to the audit site, thus saved travel and transportation time. Also, compared to human work, robot work is standardized and contains only minimal mistakes, auditors can spend less time to do the number-crunching.

Changes 4: Internal audit practices

The fourth impact will be the changes of internal audit practices. RPA allows for more uniform and efficient performance of tasks. Its work is highly traceable and auditable. Fewer manual errors are likely to occur with inherent process standardization, which improves the accuracy and audit quality (Tangent Solutions, 2020). Automation will improve compliance and lower risk up to a certain extent, and the results are often consistent and free of bias or deviation, making them reliable. On the other hand, this may also lead to a systematic mistake, where the robots would be unable to detect changes in the business environment (Gotthardt, et al., 2020).

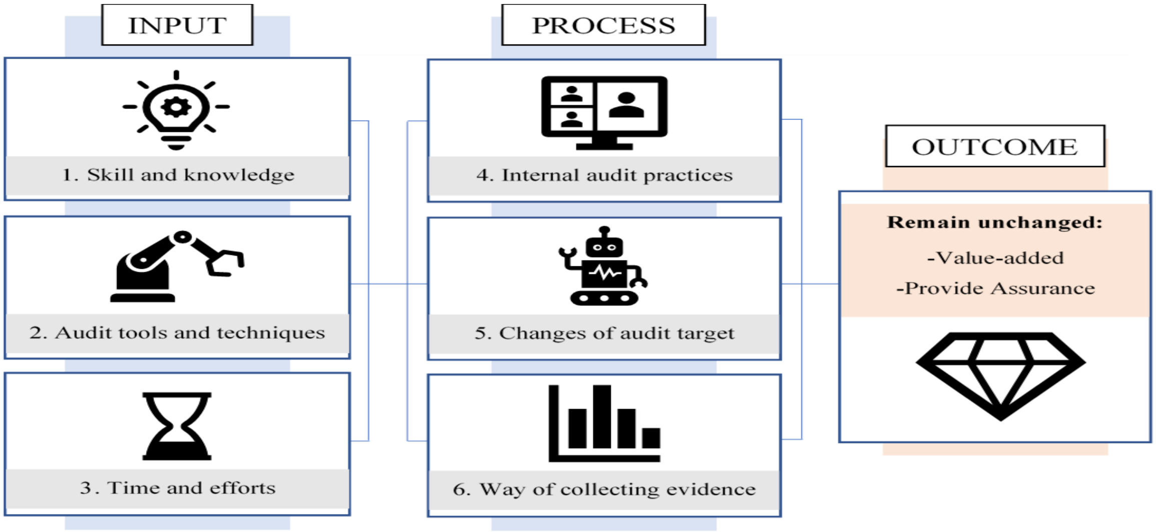
Changes 5: Audit target

When auditing in an RPA setting, the emphasis shifts from humans to robots. Rather than sample-based audits, the audit strategy would transition to more preventive controls and exception-based testing. The auditors need to evaluate whether the bot produces any exception reports that are either reviewed by management or used by the auditor in conducting audit procedures. The completeness and accuracy of data also need to be tested (Deloitte, 2018). The changes of the audit target also correspond the first construct of this study where the auditor now need to assess the risks around the robot, other than risks around the human.

Changes 6: Way of collecting evidence

For automated processes, new testing approaches are needed. Internal auditors can access the data extracted by the bot instead of requesting documents from the auditee. When auditing an attended RPA and an unattended RPA, separate audit procedures must be planned. Furthermore, by using CAATTs such as Concurrent Auditing Tools, auditors can collect audit evidence at the same time that bots process data, resulting in continuous auditing. The way of collecting audit evidence also can reflect when auditors are allowed to review RPA audit trail. According to the technical interviewees, the RPA audit trail stored every single RPA log that enabled auditors to examine the reliability of the data.

Figure 7. Proposed Framework for Changes in Internal Audit Process for Organization Deploying RPA


INPUT
1. Skill and knowledge
2. Audit tools and techniques
3. Time and efforts
PROCESS
4. Internal audit practices
5. Changes of audit target
6. Way of collecting evidence
OUTCOME
Remain unchanged:
-Value-added
-Provide Assurance

Finally, whether in terms of auditing a human-work environment, computer-based environment or RPA environment, the internal audit must first acquire a comprehensive understanding of the whole environment to better plan for audit work (ACCA, 2018). It is also mentioned by the interviewee, although there are some changes in the internal audit process, the objectives of internal audit have not changed. The IAF must assess if risks are adequately handled and provide the organization with fair assurance.

4.6.3 Research Question 3

Objective 3: To understand the skillsets required by internal auditors.

Question 3: What are the skillsets required by internal auditors?

Auditors' capabilities to audit the bot is one of the main risks area mentioned by implementation interviewees. Also, the input of internal auditors' skill and knowledge are concerned by interviewee when investigating the changes in the internal audit process. Thus it proves the significance of the third objective of this study. The third objective relates to addressing the third impact of implementing RPA on the IAF that is specifically the "skillset" required by internal auditors to audit an RPA implementation. The findings are qualitatively answered by two groups of interviewees who responded towards the research question and objective via from two perspective: implementation and technical. The interview questions for this objective were carved differently but discreetly embedded the strength to meet the research question and objective.

Skill 1: Technological competence

The first skillset identified is technological competence. As RPA supports organizational in operating day-to-day activities, internal auditors must equip with relevant technological knowledge and skills to provide reasonable assurance. To safeguard an RPA, the auditor needs to understand the used RPA platform and its core components in order to assess the risks of the RPA. He needs to be aware of how the bot is running, maintaining, securing data, the nature of the bot, and the maintenance matter.

Skill 2: IT audit skills

The second skillset required is IT audit skills. An IT auditor has a strong understanding of general computer controls, data analytics, basic system infrastructure, and risk assessment (Donathan, 2018). It also includes the competencies in utilizing audit tools and techniques or CAATTs. The extent to which auditors can employ CAATs varies, depending on the auditor's expertise (Motubatse, et al., 2015). The extensive use of IT in business today has had a significant impact on the audit profession regarding the rise of IT auditors. One of the implementation interviewees also noted that the number of IT auditors in an internal audit team would significantly increase given the rapid development of technology.

Skill 3: Business process knowledge

Internal auditors must understand the business process inherent in any business and the automated business process. They should comprehend the activities involved in each automated business process: understand the flow of that information throughout each process, and the controls over the information to ensure its integrity (Parker, 2010). When comes to RPA, even the well-designed solutions are useless if it is not set up correctly and monitored to determine whether they are performing effectively. In assisting an RPA design, the subject matter experts in business process, the internal auditors may need to advise and consult on business process improvements that can be made (Tysiac & Drew, 2018).

Skill 4: Communication skills

Communication skills have been one of the top skills that need to be equipped for an internal auditor. For a successful auditor, it means clearly conveying thoughts, ideas, and suggestions during meetings, presentations, interviews, and negotiations with audit clients and executives (Forbes and KPMG, 2018). It is evidenced that if the auditors communicate and interact well with everyone involved, the audit will be more successful. In assisting an RPA implementation, internal auditors can also act as a catalyst in convening stakeholders' requirements.

Skill 5: Competitive personalities

The fifth skillset is competitive personalities. In the wake of the turbulent global economy and its impact on financial markets and corporate viability, CAE and internal audit staff identified the competency of problem identification and solution skills, including core, conceptual, and analytical thinking (Bailey, 2010). Kokina and Blanchette (2019) also agreed that finding out the most efficient way to reduce risk is by becoming better at troubleshooting if a bot breaks.

Skill 6: Accounting and auditing

Other than that, the internal auditor must possess in-depth knowledge in accounting and auditing. Auditing skills include several specific sub-skills, such as developing and executing an audit plan, preparing and using checklists, following-up and documenting findings. Besides, it also required auditors to effectively adopt appropriate frameworks for evaluating controls and assessing technological risks. One of the interviewees highlighted the importance of internal auditing in ensuring a quality management system is effectively implemented and maintained. It is also agreed by Ohanyan and Harutyunyan (2016), who support internal audit is crucial in implementing continuous improvement of the quality management system. Internal auditing skills can assist the organization in identifying gaps in quality management and ensuring compliance and efficiency.

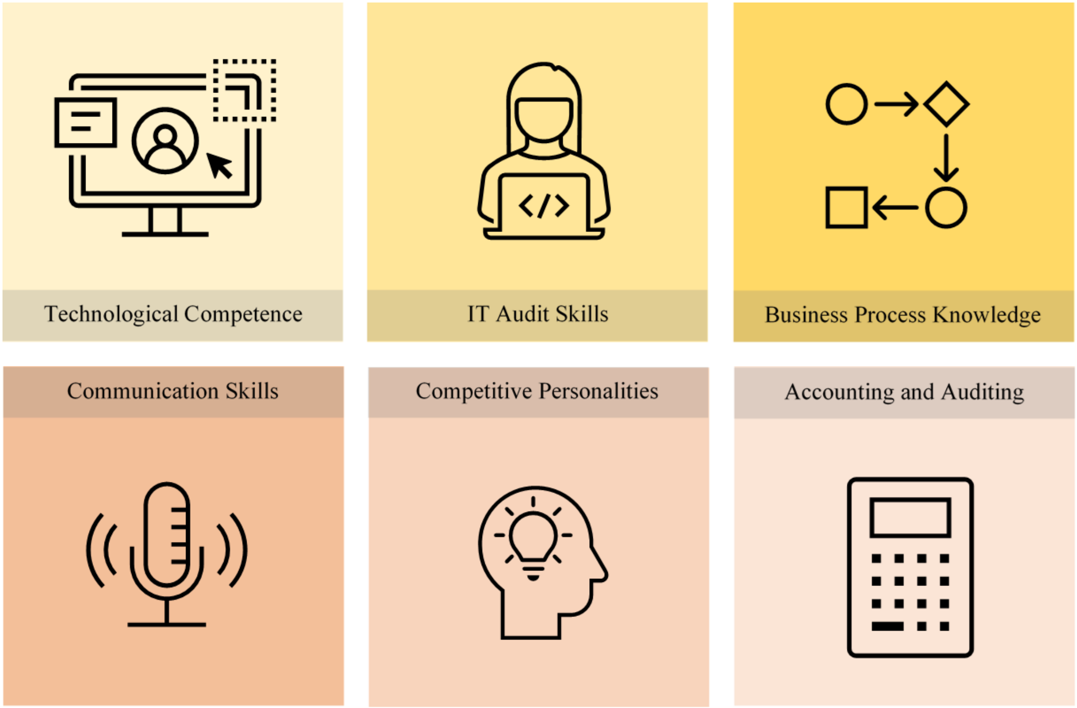


Figure 8. Proposed Framework for Skillsets Required by Internal Auditor

4.7 Solving the Research Problem

Upon answering the three research questions and meeting the three research objectives, the following paragraphs dictate how this research solve the research problem. The research problem is addressed as a theoretical gap in the study which is bound to exist due to educational issues. The educational issues in this study revolve around **three important dimensions**: key risk areas within an RPA implementation, changes in the internal audit process and skillset required by the internal auditors.

Based on the merged implementation and technical responses that answered and met research questions and objectives 1, it clearly fills the gap by solving the first educational issues. As RPA is an emerging technology, there has been no study that have specifically identified key risk areas within an RPA implementation. The identification of key risk areas within an RPA implementation is imperative to spread the necessary understanding and awareness to internal auditor in the advent of IR4.0 where automation and RPA appears to extend at unprecedented scale. ***Thus, this study is carried out to bridge the gap by identifying and proposing a framework for nine key risk areas within RPA implementation.***

Based on the merged implementation and technical responses that responded and fulfil research question and objectives 2, it clearly fills the gap by solve the second educational issues. Internal auditors need to be better prepared to define a new audit plan when auditing an RPA environment. This study collected point of views from experienced practitioners from the field of internal and IT auditing to pertain the view regarding the changes in the internal audit process when comes to auditing a bot. The argument also supported by technical personnel who urged the need of transformation of the internal audit process to audit RPA. ***Thus, this study is carried out to bridge the gap by investigating and proposing a framework for the six changes in the internal audit process for organization undertaking RPA.***

Based on the merged implementation and technical responses that reflected and satisfied research question and objective 3, it clearly fills the gap by solve the third educational issues.

Particularly, this research explores the skillset required by the internal auditor to audit an RPA system. Auditors need to rethink to brush up their skill in this highly demanding and rapidly changing landscape. ***Thus, this study is carried out to bridge the gap by understanding and proposing a framework for six skillsets required by internal auditor.***

4.8 Conclusion

In this chapter, the purpose of the interview questions and the themes extracted from both implementation and technical responses have been discussed. The discussion from both implementation and technical indicators were merged to related, connected, and explain the results. Upon merging, the findings manifested from the discussion strongly answered the research questions, satisfy research objectives and finally solving the research problem. To make it more clear for the reader to understand, the study proposed three frameworks for answer the three research questions, respectively.

5 Conclusion, Implications, Limitations and Recommendations

This chapter involves the process of meditating the results and findings of the study to clarify the feasibility of the results and findings towards the research objectives. This is because it is only by introspection that the shortcomings encountered can be fully understood and inspired to turn them into real solutions that can be offered to the universe, so that more research can be carried out to combat the limitations. This chapter also offers the ability for the author to present the final say of this study.

5.1 Research Purpose Evaluation

In line with objective 1, it is evident that RPA has impact to the IAF, in terms of introducing new risks to the organization. It clearly fills the research gap by identified nine key risk areas within an RPA implementation: right of access, data protection and security, technical risks, auditor's capabilities, change management risks, nature of the bot, operation and executive risks, intervention of human, ROI of RPA.

In line with objective 2, it is evident that RPA has impact to the IAF, in terms of transforming the internal audit process. It clearly fills the research gap by identified six changes in the internal audit process for an organization undertaking RPA: inputs of skill and knowledge, audit tools and techniques, input of time and efforts, internal audit practices, changes of audit target and way of collecting evidence.

In line with objective 3, it is evident that RPA has impact to the IAF, in terms of demanding new skillset of internal auditor. It clearly fills the research gap by identified six skillsets required by the internal auditor when auditing RPA: technological competence, IT audit skills, business process knowledge, communication skills, competitive personalities and accounting and auditing.

This study was deemed satisfactory as all of the research questions were answered. The relevance of the research findings towards the research objectives satisfied the ultimate goals of this study, which is to provide a complete understanding of the phenomenon of **"The Impact of Implementing Robotic Process Automation on the Internal Audit Function"**.

5.2 Recommendation

Upon implementation of an automated environment, organization must scale their automation to fully utilize the benefits of RPA and promotes the RPA growth. UiPath (2019) introduced a seven-pillar framework that can help companies define and solve challenges within an RPA implementation, as well as develop an automation strategy. The first pillar **(Pillar 1: Executive visioning)** mandated organizations to have ongoing executive support in order to establish and articulate a vision that would direct them through the entire automation journey. The vision must be born out of the intersection of business objectives and technological possibilities. The second pillar **(Pillar 2: Automation operating model)** required organizations to develop an automation operating model to support RPA implementation, scaling and transformation across SDLC. Create a CoE to handle change management for long-term transformation, and re-skill the workforce so they can concentrate on higher-value tasks. The third pillar **(Pillar 3: Value creation and assurance)** and the fourth pilar **(Pillar 4: Business outcome prioritization)** allowed organization to prioritize value creation over cost reduction. The fifth pillar **(Pillar 5: IT automation readiness)** necessitated earlier IT involvement. The sixth pillar **(Pillar 6: Control framework)** guided organizations to establish a control environment that complies with Sarbanes-Oxley Act, the General Data Protection Regulation, and other related regulation. The last pillar **(Pillar 7: Citizen model and attended strategy)** reviewed the previous pillars and concentrated on creating an attended robot strategy that benefited from citizen developers.

To establish a robust RPA control environment, especially as organizations scale the number of bots in operation, RPA-specific preventive controls and thorough documentation including coding best practices must be developed. To design the controls as part of RPA implementation, the IAF should engage in SDLC and lean management. RPA required a new understanding of risk and internal controls. The use of RPA does not increase overall risk within an organization as long as appropriate internal controls are put in place. Furthermore, profiling bot risk levels and establishing preventative controls are an essential part of the RPA control framework. An organization undertaking RPA must have robust security and compliance in place.

The impact of RPA on the IAF is also reflected in terms of changes in the internal audit process. To auditing a bot, auditors need to have new methodologies, updated tools, and appropriate resources to ensure the risks and controls of RPA are reasonably assured. Planning for audit engagement is the most critical step during an audit engagement; an audit engagement must be equipped with appropriate and sufficient resources. Since internal audit interfaces with several departments and audits several processes within an organization, it can help identify an opportunity to embed automation-enabled control activities within the business processes. The auditing concept to ensure the controls are in place and risks are controls is remained; the changes will only be the resources and methodologies that the auditor used for auditing. To embody the value of internal auditing, the auditor can also adopt advanced technologies to increase efficiency and improve audit quality.

Auditors need to update their skillset while remaining their core competencies continually. Given the new risks and internal audit procedures introduced to cope with the RPA environment, auditors have to upskill themselves to audit such complex environments. The proposed skillsets in this study are not limiting in auditing an RPA environment; it is also capable when auditing in any technology environment. From this study, it can be seen that the emerging technologies have a significant impact on the internal audit profession, especially comes to the ability of the auditor to control and utilized them.

5.3 Further Research

Based on the research performed, several areas surfaced:

- RPA as CAATTs: What challenges arise for an internal auditor to adopt RPA as an audit tool? How can RPA be used by the internal auditor to increase the audit quality? What tools are the most promising?
- Control considerations of implementing RPA: How the risks arising from the implementation of RPA can be controlled? How should the challenges be addressed?
- Data protection of RPA: How is the RPA data privacy ensured? What are the challenges expected when it comes to RPA data protection and privacy?
- RPA governance: What governance should be in place in an RPA environment? What is the impact of implementing RPA on organizational governance?

- Process improvement: How RPA promotes process improvement?
- RPA and Continuous Auditing: How RPA can realize continuous auditing? How can the IAF utilize RPA in realizing continuous auditing?
- RPA and other tools: How RPA can integrate with other tools and technologies?

5.4 The Final Note

This research "The Impact of Implementing Robotic Process Automation on the Internal Audit Function: a Malaysian study" definitely tickles the mind to show interest pertaining the effect behind the selection of these particular set of terminologies. This study explores the impact of RPA on the IAF in terms of three areas: key risk area, changes in internal audit process and skillset required by the internal auditor. It is directed to all professionals, but auditor, internal auditor and IT auditor more specifically, as they need to aware of the impact introduced by the RPA.

References

Abdolmohammadi, M. J. & Boss, S. R. (2010). Factors associated with IT audits by the internal audit function. International Journal of Accounting Information Systems, 11(3), pp. 140-151.

ACCA. (2018). Auditing in a computer-based environmen. [Online] Available at: https://www.accaglobal.com/hk/en/student/exam-support-resources/professional-exams-study-resources/p7/technical-articles/auditing-computer-based-environment2.html [Accessed 28 February 2021].

Aggranda. (2020). About us. [Online] Available at: https://www.aggranda.com/ [Accessed 10 February 2021].

Aguirre, S. & Rodriguez, A. (2017). Automation of a Business Process Using Robotic Process Automation (RPA): A Case Study. Applied Computer Sciences in Engineering, pp. 65-71.

Amirudin, I. (2021). Industry 4.0: Spurring productivity through RPA. [Online] Available at: https://www.theedgemarkets.com/article/industry-40-spurring-productivity-through-rpa [Accessed 27 February 2021].

Austion, Z. & Sutton, J. (2015). Qualitative Research: Data Collection, Analysis, and Management. The Canadian Journal of Hospital Pharmacy, 68(3), pp. 226-231.

Bahador, K. M. K. & Haider, A. (2015). Skillset to Assimilate Information Technologies in Accounting SMEs. Business Technologies in Contemporary Organizations: Aoption, Assimilation, and Institutionalization. United States: IGI Global, p. 35.

Bailey, J. A. (2010). Core Competencies for Today's Internal Auditor. The Institution of Internal Auditors Research Foundation.

Barac, K., Gammie, E., Howieson, B. & Staden, M. V. (2016). The Capability and Competency Requirements of Auditors in Today's Complex Global Business Environment. The Institute of Chartered Accountants of Scotland (ICAS) and The Financial Reporting Council (FRC).

Bendor-Samuel, P. (2018). RPA Study Reveals Difficulties in Achieving ROI | Sherpas in Blue Shirts. [Online] Available at: https://www.everestgrp.com/2018-06-rpa-study-reveals-difficulties-achieving-roi-sherpas-blue-shirts-45492.html/ [Accessed 22 February 2021].

Bierstaker, J. L., Burnaby, P. & Thibodeau, J. (2001). The Impact Of Information Technology On The Audit Process: An Assessment Of The State Of The Art And Implications For The Future. Managerial Auditing Journal, 16(3), p. 159.

Blue Print. (2020). How to Reduce the Rising Costs of RPA Maintenance and Support. [Online] Available at: https://www.blueprintsys.com/blog/rpa/reduce-rising-costs-rpa-maintenance-and-support [Accessed 26 February 2021].

Blue Prism. (2018). Coca-Cola extends business services capacity and improved performance with RPA. [Online] Available at: https://www.blueprism.com/uploads/resources/case-studies/blue-prism-cola-case-study.pdf [Accessed 4 October 2020].

Brachio, A. (2021). How internal audit can help make RPA implementation a success. [Online] Avilable at: https://www.ey.com/en_gl/consulting/how-internal-audit-can-help-make-rpa-implementation-a-success [Accessed 10 March 2020].

Brent D. Slife, C. D. W. & Yanchar, S. C. (2016). Using Operational Definitions in Research: A Best-Practices Approach. The Journal of Mind and Behavior, 37(2), pp. 119-139.

Bryan, J. (2019). Why Audit Leaders Need to Adopt RPA. [Online] Available at: https://www.gartner.com/smarterwithgartner/why-audit-leaders-need-to-adopt-rpa/ [Accessed 21 August 2020].

Cacciattolo, M. (2015). Ethical Considerations in Research. In: M. Cacciattolo, ed. Ethical Considerations in Research. Rotterdam: Sense Publishers, pp. 61-79.

Capgemini. (2019). Have you considered the risks and controls before implementing RPA?. [Online] Available at: https://www.capgemini.com/2019/01/have-you-considered-the-risks-and-controls-before-implementing-rpa/ [Accessed 16 February 2021].

Carr, D. F. (2020). Robotic Process Automation (RPA) careers: 4 hot job titles. [Online] Available at: https://enterprisersproject.com/article/2020/2/rpa-robotic-process-automation-4-hot-job-titles [Accessed 27 February 2021].

Celonis (2017). 3 Critical Steps to make your RPA implementation a success. Celonis.

Cewe, C., Koch, D. & Mertens, R. (2017). Minimal Effort Requirements Engineering for Robotic Process Automation with Test Driven Development and Screen Recording. Business Process Management, pp. 642-648.

Chambers, A. D. & Odar, M. (2015). A new vision for internal audit. Managerial Auditing Journal, 30(1), pp. 34-55.

Chau, H. (2019). The Opportunities in Enterprise RPA. [Online] Available at: https://venturebeat.com/2019/07/28/the-opportunities-in-enterprise-rpa/ [Accessed 27 February 2021].

Chuah, H. & Maes, T. (2016). Technology-Enabled Internal Audit. [Online] Available at: https://www.compact.nl/en/articles/technology-enabled-internal-audit/#ref [Accessed 21 July 2020].

CIMB. (2017). Robotic Reduce CIMB's Turnaround Time For Banking Tasks By Up To 90%. [Online] Available at: https://www.cimb.com/en/newsroom/2017/robotics-reduce-cimbs-turnaround-time-for-banking-tasks-by-up-to-90.html [Accessed 4 October 2020].

Cohen, M., Rozario, A. M. & Zhang, C. (2019). Exploring the Use of Robotic Process Automation (RPA) in Substantive Audit Procedures. [Online] Available at: https://www.cpajournal.com/2019/08/14/exploring-the-use-of-robotic-process-automation-rpa-in-substantive-audit-procedures/#:~:text=RPA%20can%20streamline%20audit%20evidence,as%20Excel%20or%20CaseWare%20IDEA%20([Accessed 5 August 2020].

Cooper, L., Holderness, K., Sorensen, T. & Wood, D. A. (2019). Robotic Process Automation in Public Accounting. Accounting Horizons, 33(4), pp. 15-35.

DeBrush, C. (2017). Five Robotic Process Automation Risks to Avoid. [Online] Available at: https://sloanreview.mit.edu/article/five-robotic-process-automation-risks-to-avoid/ [Accessed 26 February 2021].

DeCarlo, M. (2018). 9.3 Operationalization. In: Scientific Inquity in Social Work. Open Social Work Education, pp. 235-242.

Dejonckheere, M. & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: a balance of relationship and rigour. Family Medicine and Community Health, 7(2).

Deloitte. (2018). Auditing the RPA environment : Our Approach Towards Addressing Risks in a BOT Environment. [Online] Available at: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-auditing-the-rpa-environment-noexp.pdf [Accessed 1 October 2020].

Devarajan, Y. (2018). A Study of Robotic Process Automation Use Cases Today for Tomorrow's Business. International Journal of Computer Techniques, 5(6), pp. 12-18.

DiCicco-Bloom, B. & Crabtree, B. F. (2006). The qualitative research interview. Medical Education, Volume 40, pp. 314-321.

Digital Workforce (2020). Measuring RPA ROI - How to do it right?. [Online] Available at: https://digitalworkforce.com/rpa-news/measuring-rpa-roi-how-to-do-it-right/ [Accessed 17 February 2021].

Donathan, C. (2018). So You Want to Be an IT Auditor?, The Institute of Internal Auditors.

Duncan, B. & Whittington, M. (2016). Enhancing Cloud Security and Privacy: The Cloud Audit Problem. Cloud Computing 2016, pp. 119-124.

Dworkin, S. L. (2012). Sample Size Policy for Qualitative Studies Using In-Depth Interviews. Archives of Sexual Behavior, Volume 41, pp. 1319-1320.

Electroneek. (2020a). RPA and VBA Dilemma: Why Do I Need Robotics When I Have Macros?. [Online] Available at: https://electroneek.com/blog/technology-insights/rpa-and-vba-dilemma-why-do-i-need-robotics-when-i-have-macros/ [Accessed 1 March 2021].

Electroneek. (2020b). Security Concerns in RPA: 4-Step Guide to Address Them. [Online] Available at: https://electroneek.com/blog/technology-insights/security-concerns-in-rpa-4-step-guide-to-address-them/ [Accessed 22 February 2021].

Epicor. (2020). What is Industry 4.0—the Industrial Internet of Things (IIoT)?. [Online] Available at: https://www.epicor.com/en-ae/resource-center/articles/what-is-industry-4-0/ [Accessed 28 July 2020].

Ernst & Young LLP. (2017). Get ready for Robotic Process Automation. [Online] Available at: https://www.ey.com/en_qa/financial-services-emeia/get-ready-for-robotic-process-automation [Accessed 26 February 2021].

Ernst & Young LLP. (2018). ISACA LA November 2018 : Robotics Process Automation (RPA) and Artificial Intelligence (AI): A New World Order.

European Court of Auditors. (2020). Smart Audit: the digital transformation of audit. [Online] Available at: https://medium.com/ecajournal/smart-audit-the-digital-transformation-of-audit-b283e1653bd4 [Accessed 10 August 2020].

Federal RPA Community of Practice. (2020). Creating a Robust Controls Systems for RPA Programs. [Online] Available at: https://digital.gov/pdf/rpa-playbook-ic-addendum-v1.0.pdf [Accessed 23 September 2020].

Fernando, L. (2020). Business Process Standardization With RPA. [Online] Available at: https://medium.com/@lahirufernando90/business-process-standardization-with-rpa-fe626f1f2a9f [Accessed 17 February 2021].

Fersht, P. (2018). RPA is officially the shiny new silver bullet: 53% of the Global 2000 are planning significant RPA investments to slash costs in 2018. [Online] Available at: https://www.horsesforsources.com/RPAglobal2000_031118 [Accessed 25 August 2020].

Figueroa-Garcia, J. C., Lopez-Santana, E. R., Villa-Ramirez, J. L. & Ferro-Escober, R. (2017). Applied Computer Sciences in Engineering. Communications in Computer and Information Science.. Colombia, Workshop on Enginerring Applications.

Firouzi, H. O. & Wang, S. (2020). A Fresh Look at Internal Audit Framework at the Age of Artificial Intelligence (AI). Toronto Dominion Bank.

Forbes and KPMG. (2018). Five Skills Auditors Need To Succeed Today. [Online] Available at: https://www.forbes.com/sites/insights-kpmg/2018/07/16/five-skills-auditors-need-to-succeed-today/?sh=4bc106992356 [Accessed 24 February 2021].

Francis, J. J. et al. (2010). What is an adequate sample size? Operationalising data saturation for theory-based interview studies. Psychol Health, 25(10), pp. 1229-1294.

Gadre, A., Jessel, B. & Gulati, K. (2017). Rethinking Robotics? Take a Step Back. The Capco Institute Journal of Financial Transformation, Automation(3), pp. 34-45.

Gartner. (2018). Robotic Process Automation: Implications for Internal Audit. Gartner Inc.

Giesbers, S. (2020). Robotic Process Automation and internal control: A guideline, Amsterdam: Vrije Universiteit Amsterdam.

Globaldata.com. (2020). APAC set to emerge as epicenter for artificial intelligence growth, says GlobalData. [Online] Available at: https://www.globaldata.com/apac-set-to-emerge-as-epicenter-for-artificial-intelligence-growth-says-globaldata/ [Accessed 3 October 2020].

Gotthardt, M. et al. (2020). Current State and Challenges in the Implementation of Smart Robotic Process Automation in Accounting and Auditing. ACRN Journal of Finance and Risk Perspectives, Volume 9, pp. 90-102.

Gray, J. M. (2016). Information Technology Audits by Internal Auditors: Exploring the Evolution of Integrated IT Audits, United States: Bentley University.

Gutierrez, C. (2018). Zurich Insurance Group Incorporates RPA to Achieve $1B of Savings. [Online] Available at: https://www.altoros.com/blog/zurich-insurance-group-incorporates-rpa-to-achieve-1b-of-savings/ [Accessed 4 October 2020].

Hass, S., Abdolmohammadi, M. J. & Burnaby, P. (2006). The Americas literature review on internal auditing. Managerial Auditing Journal, 21(8), pp. 825-844.

Havelka, D. & Merhout, J. W. (2013). Internal information technology audit process quality: Theory development using structured group processes. International Journal of Accounting Information Systems, 14(3), pp. 165-192.

Herm, L.-V.et al. (2020). A Consolidated Framework for Implementing Robotic Process Automation Projects. In: Fahland D., Ghidini C., Becker J., Dumas M. (eds) Business Process Management. BPM 2020. Lecture Notes in Computer Science, Volume 12168, pp. 471-488.

Héroux, S. & Fortin, A. (2013). The Internal Audit Function in Information Technology Governance : A Holistic Perspective. Journal of Information Systems, 27(1), pp. 189-217.

Hofmann, P., Samp, C. & Urbach, N. (2020). Robotic process automation. Electronic Market, Volume 30, pp. 99-106.

Horvath, I. (2020). Top Risk Management Frameworks. [Online] Available at: https://www.invensislearning.com/blog/risk-management-frameworks/ [Accessed 11 February 2021].

Huang, F. & Vasarhelyi, M. A. (2019). Applying robotic process automation (RPA) in auditing: A framework. International Journal of Accounting Information Systems, Volume 35, p. 100433.

IAASB. (2014). Key Elements that Create An Environment For Audit Quality. The International Auditing and Assurance Standards Board.

ICAEW. (2018). How do you audit a robot?. [Online] Available at: https://www.icaew.com/technical/business-and-management/strategy-risk-and-innovation/risk-management/internal-audit-resource-centre/how-do-you-audit-a-robot [Accessed 2 March 2021].

ICAEW. (2019). Three Lines of Defense Review. [Online] Available at: https://www.icaew.com/-/media/corporate/files/technical/icaew-representations/2019/icaew-rep-94-19-three-lines-of-defence-review.ashx [Accessed 1 October 2020].

IEEE Corporate Advisory Group. (2017). IEEE Guide for Terms and Concepts in Intelligent Process Automation. New York City: IEEE.

IIA. (2004). What is Internal Auditing. [Online] Available at: https://www.iia.org.uk/about-us/what-is-internal-audit [Accessed 23 September 2020].

IIA. (2012). Auditing IT Governance. [Online] Available at: http://194.177.36.87/IFACI/GTAG%2017_Auditing_IT_Governance_2012.pdf [Accessed 2 October 2020].

IIA. (2013). The Three Lines of Defense In Effective Risk Management and Control. [Online] Available at: https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf [Accessed 22 September 2020].

IIA. (2017). Robotic Process Automation (RPA) - The Impact on Internal Audit. [Online] Available at:https://chapters.theiia.org/sandiego/Documents/Presentations/RPA%20IIA%20Presentation%20San%20Diego.pdf [Accessed 2 October 2020].

IIA. (2019). Code of Ethics. The Institute of Internal Auditors.

IIA. (2020). Why Audits Take Longer Than The Time Allocated. The Institute of Internal Auditors.

Infosys. (2020). Security Considerations in Robotic Process Automation. [Online] Available at: https://www.infosys.com/services/cyber-security/documents/rpa-security.pdf [Accessed 2 October 2020].

Intelligence, P. (2020). Robotic Process Automation Market Overview. P&S Intelligence.

ISG. (2020. Don’t Overlook the Risk Posed by Robots. [Online] Available at: https://isg-one.com/articles/don-t-overlook-the-risk-posed-by-robots [Accessed 26 February 2021].

Jamshed, S. (2014). Qualitative research method-interviewing and observation. Journal of Basic and Clinical Pharmacy, 5(4), p. 87.

Joshi, N. (2019). Leverage RPA, But Plan For Its Inherent Risks, Too!. [Online] Available at: https://www.forbes.com/sites/cognitiveworld/2019/06/28/leverage-rpa-but-plan-for-its-inherent-risks-too/?sh=2841df811d17 [Accessed 22 February 2021].

Kaya, C. T., Turkyilmaz, M. & Birol, B. (2019). Impact of PRA Technologies on Accounting Systems. The Journal of Accounting and Finance, Volume 82, pp. 235-250.

Kokina, J. & Blanchette, S. (2019). Early evidence of digital labor in accounting: Innovation with Robotic Process Automation. International Journal of Accounting Information Systems, pp. 1-13.

Kovanen, A. (2020). Risks of Intelligent Automation and Their Impact on Internal Audit, Finland: Tampere University.

KPMG. (2018). Internal Audit and Robotic Process Automation. [Online] Available at: https://assets.kpmg/content/dam/kpmg/nl/pdf/2018/advisory/part-2-internal-audit-and-robotic-process-automation.pdf [Accessed 1 October 2020].

Lacity, M. C. & Willcocks, L. P. (2016). A New Approach to Automating Services. [Online] Available at: https://sloanreview.mit.edu/article/a-new-approach-to-automating-services/ [Accessed 2 Obtober 2020].

Lacity, M. C, & Willcocks, L. P. (2017). Robotic Process Automation and Risk Mitigation : The Definitive guide. 1st ed. Ashford: SB Publishing.

Lois, P., Drogalas, G. & Karagiorgos, A. (2020). Internal Audits in the Digital Era: Opportunities Risks and Challenges. EuroMed Journal of Business, 15(2), pp. 205-217.

Mack, N. et al. (2005). Qualitative Research Methods: A Data Collector's Field Guide. 1st ed. North Carolina: Family Health International.

Mac, R. (2019). Automating Processes in Excel: Part 1 Why RPA is not VBA. [Online Available at: https://www.ashlingpartners.com/why-rpa-is-not-vba/ [Accessed 1 March 2021].

Madakam, S., Holmukhe, R. M. & Jaiswal, D. K. (2019). The Future Digital Work Force: Robotic Porcess Automation (RPA). Journal of Information Systems and Technology Management, Volume 16.

Magee, K. (2018). IT Auditing and Controls – Planning the IT Audit. [Online] Available at: https://resources.infosecinstitute.com/itac-planning/#gref [Accessed 23 September 2020].

Maybank (2018). Annual report 2018, Malaysia: Maybank.

Miles, M. B., Huberman, A. M. & Saldaña, J. (2014). Matthew B. Miles, A. Michael Huberman, and Johnny Saldaña. 3rd ed. Thousand Oaks: SAGE Publication.

Moayed, V. (2018). RPA and the ROI Conundrum. [Online] Available at: https://www.uipath.com/blog/rpa-and-the-roi-conundrum [Accessed 19 February 2021].

Moeller, R. (2010). IT Audit, Control, and Security. 1st ed. United Stated of America: John Wiley & Sons.

Moffitt, K. C., Rozario, A. & Vasarhelyi, M. A. (2018). Robotic Process Automation for Auditing. Journal of Emerging Technologies in Accounting, 15(1), pp. 1-10.

Moorthy, M. K. et al. (2011). The impact of information technology on internal auditing. Journal of Business Management, 5(9), pp. 3523-3539.

Motubatse, K. N., Staden, M. v., Steyn, B. & Erasmus, L. (2015). Audit Tools and Techniques: Crucial Dimensions of Internal Audit Engagements in South Africa. J Economies, 6(3), pp. 269-279.

Ohanyan, A. & Harutyunyan, H. (2016). The Role of Internal Audit in Continuous Improvement of Quality Management Systems at Private HE Institutions: A Case Study of Eurasia International University (Armenia). Journal of Business & Financial Affairs, 5(1), pp. 1-10.

Parker, R. G. (2010). Business Skills for the IT Audit and Assurance Professional. ISACA JOURNAL ARCHIVES.

Pawlowski, J. (2019). Deploying Digital Labor in Internal Auditing by Introducing and Utilizing Robotic Process Automation. Southern California, The Institute of Internal Auditor International Conference .

Petters, J. (2021). Risk Management Framework (RMF): An Overview. [Online] Available at: https://www.varonis.com/blog/risk-management-framework/ [Accessed 26 February 2021].

Pluzhnikov, O. (2021). Top 10 Security Risks of RPA. Eleks.

Pritzker, M. D. (2020). What are the limitations of RPA?. [Online] Available at: https://www.itcentralstation.com/questions/what-are-the-limitations-of-rpa [Accessed 17 February 2021].

Priyadarshi, G. (2019). Inherent Risk in Adopting RPA and Opportunities for Internal. [Online] Available at: https://www.isacajournal-digital.org/isacajournal/2019_volume_6/MobilePagedArticle.action?articleId=1534862#articleId1534862 [Accessed 18 February 2021].

PwC. (2017a). Robotic process automation : A primer for internal audit professionals. [Online] Available at: https://www.pwc.com/us/en/risk-assurance/publications/assets/pwc-robotics-process-automation-a-primer-for-internal-audit-professionals-october-2017.pdf [Accessed 21 July 2020].

PwC. (2017b). A Leading IT Internal Audit Function through the lens of a CIO, US: PwC.

PwC. (2019). Re-inventing Internal Controls in the Digital Age. [Online] Available at: https://www.pwc.com/sg/en/publications/assets/reinventing-internal-controls-in-the-digital-age-201904.pdf [Accessed 28 August 2020].

Ramamoorti, S. & Weidenmier, M. L. (2004). The Pervasive Impact of Information Technology on Internal Auditing. The IIA Research Foundation.

Rissi, J. & Sherman, S. (2011). Cloud-Based IT Audit Process.. New York: John Wiley & Sons.

Rodrigues, V., Cunha, D. & Reznik, M. (2020). RPA Governance. [Online] Available at: https://visagio.com/en/insights/rpa-governance-automating-processes-efficient-sustainable-manner [Accessed 1 March 2021].

Romao, M., Costa, J. & Costa., J. C. (2019). Robotic Process Automation: A Case Study in the Banking Industry. 14th Iberian Conference on Information Systems and Technologies.

Roy, G. (2020). RPA Security Must-Haves. [Online] Available at: https://www.automationanywhere.com/company/blog/learn-rpa/rpa-security-must-haves [Accessed 26 February 2021].

SAGE. (2019). Thematic Analysis of Interview Data in the Context of Management Controls Research. SAGE Publications.

Saharia, A., Koch, B. & Tucker, R. (2008). ERP Systems and Internal Audit. Issues in Information Systems, 9(2), pp. 578-586.

Salmons, J. (2012). Designing and Conducting Research with Online Interviews. In: Cases in Online Interview Research. SAGE Publications, pp. 1-30.

Santos, F., Pereira, R. & Vasoncelos, J. B. (2019). Towards Robotic Porcess Automation. Business Proces Management Journal, 26(2), pp. 405-420.

Schuett, M. (2019). Robotic Process Automation Meets Identity and Access Management. Information System Security Association (ISSA).

Singh, V. K. (2019). Types of Exception in blue prism. [Online] Available at: https://dotnetbasic.com/2019/04/types-of-exception-in-blue-prism.html [Accessed 19 February 2021].

Soh, D. S. B. & Martinov-Bennie, N. (2011). The internal audit function: Perceptions of internal audit roles, effectiveness and evaluation. Managerial Auditing Journal, 26(7), pp. 605-622.

Srinivasan, V. (2017). The Intelligent Enterprise In The Era of Big Data. New Jersey: John Wiley & Sons.

Statistics Solutions (2015). Qualitative Sampling Techniques. [Online] Available at: https://www.statisticssolutions.com/qualitative-sampling-techniques/ [Accessed 6 October 2020].

Struthers-Kennedy, A. (2018). RPA: First Steps to Greater Internal Audit Efficiency. [Online] Available at: https://www.corporatecomplianceinsights.com/rpa-first-steps-to-greater-internal-audit-efficiency/ [Accessed 2 October 2020].

Tangent Solutions (2020). The Reshaping of Internal Audit through Robotic Process Automation. [Online] Available at: https://tangentsolutions.co.za/articles/reshaping-of-internal-audit/ [Accessed 24 February 2021].

Tan, J. Y. (2019). Capgemini picks Malaysia for Robotic Process Automation CoE. [Online] Available at: https://www.digitalnewsasia.com/digital-economy/capgemini-picks-malaysia-robotic-process-automation-coe [Accessed 4 October 2020].

The Institute of Chartered Accountants of India. (2018). Audit In an Automated Environment. In: Auditing and Assurance. The Institute of Chartered Accountants of India, pp. 6.1-6.26.

Tolly, K. (2019). RPA security best practices include access control, system integration. [Online] Available at: https://searchsecurity.techtarget.com/tip/RPA-security-best-practices-include-access-control-system-integration [Accessed 16 February 2021].

Turner, R. (2019). Securing Robotic Process Automation is the new business priority. [Online] Available at: https://technative.io/securing-robotic-process-automation-is-the-new-business-priority/ [Accessed 22 February 2021].

Tysiac, K. & Drew, J. (2018). 4 skills accountants need to succeed in a tech-enabled future. [Online] Available at: https://www.journalofaccountancy.com/issues/2018/jun/technology-skills-for-accountants.html [Accessed 24 February 2021].

UiPath. (2017). Robotic Process Automation (RPA). [Online] Available at: https://www.uipath.com/rpa/robotic-process-automation [Accessed 22 September 2020].

UiPath. (2019). Scale Your Automation Program with This 7-Pillar Framework. [Online] Available at: https://www.uipath.com/blog/framework-scaling-automation-programs [Accessed 2 March 2021].

UiPath. (2020a). Attended, Unattended and Hybrid: 6 Flexible Automation Deployment Models to Get the Most from RPA. UiPath.

UiPath (2020b). Robotic Process Automation and IT Compliance. UiPath.

Vasileiou, K., Barnett, J., Thorpel, S. & Young, T. (2018). Characterising and justifying sample size sufficiency in interview-based studies: systematic analysis of qualitative health research over a 15-year period. BMC Medical Research Methodology, Volume 18, p. 148.

Walter, A. (2019). The Dark Side of Robotic Process Automation. [Online] Available at: https://www.cio.com/article/3433181/the-dark-side-of-robotic-process-automation.html [Accessed 26 February 2021].

Willcocks, L., Lacity, M. & Craig, A. (2015). The IT Function and Robotic Process Automation. [Online] Available at: http://eprints.lse.ac.uk/64519/1/OUWRPS_15_05_published.pdf [Accessed 2 October 2020].