Resolving Pressure and Stress on Governance Models from Robotic Process Automation Technologies

William H. Money
Management and Entrepreneurship Department
Tommy and Victoria Baker School of Business
The Citadel
Charleston, South Carolina, USA

Abstract

Technology applications and wide exploitation of technology are the objectives of many resource utilization and time saving improvements. These programs are traditionally managed by information resource management organizations in the same fashion as other ongoing technology programs. However, a relatively new technology, robotic process automation (RPA), has been posited to add increasing complexity that stresses the governance approaches of newly adopting organizations because this technology's capabilities do not fit well into the traditional governance approaches, and control areas. Information resource management organizations and executives must therefore carefully assess how governance is provided and implemented for this technology. Careful analysis is needed to balance the organizational demands and pressures for the application of the technology against the potential risks and concerns, and safely permit wide use of the RPA technology. The risks and problem for RPA arises from the basic governance concepts of implementing security, configuration and performance controls while enabling organizations to innovate and capture the benefits of the new technology. Governance models are problematic to apply and may not address all of the features of RPA. This paper provides an overview of information technology (IT) governance, reviews the RPA technology, and contrasts RPA with the applicable governance components of one of the key IT governance models. Government, industry, and vendor published data do not provide clear recommendations for RPA governance models and approaches. This paper assessed RPA requirements, and a prominent governance model and found no strong rationale for developing new governance models or frameworks for the RPA technology. This paper suggests that features and issues that address the differences between current information systems and information technologies and RPA can be incorporated into the current governance models. This paper recommends a deep analysis of the application opportunities and risks associated with RPA utilization, and that current models of governance be adapted to fully assess the RPAs tools that are incorporated into user applications and environments.

Keywords: Governance, Technology, Robotic Process Automation, Data Governance, Security

1. INTRODUCTION

Information technology (IT) governance is important from many perspectives. Stakeholder, including users, managers, executives, funding authorities, and technical staff support governance objectives to ensure effective IT solutions. From a high-level oversight framework, governance ensures that data and reporting accurately reflect and "prove" corporate compliance with requirements, and uphold general progress in its security efforts. From an end-user or low level IT implementation and user perspective, governance ensures that the technology can be acquired, supported, installed and used without excessive costs or disruption to work.

At the high enterprise decision levels, resources must be applied wisely to assure they support the strategic objectives of an organization. At the client (user) level, data governance, and enterprise management practices will ensure that data are not lost, and the user data are not compromised. The importance of effective governance can be illustrated by describing the damage from the case of a large data breach reported in an incident handling case study of Equifax. It was a massive breach of sensitive personal and financial information. Data released included: social security numbers, birth dates and addresses, and in some cases driver license numbers, credit card information and financial dispute documents of over 140 million persons. This data release represented over 44% of the U.S. population. This company was trusted with handling and carefully securing all records (Wang & Johnson, 2018). The economic losses for the company, credibility losses for management, and user costs from this single event were enormous.

Approaches to IT Governance

Governance follows several different pragmatically established models in various industries. For example, in healthcare, the governance models seek to do similar things including providing data for complex, non-routine decisions. Governance controls require individuals, committees, and processes ensure that the organizational strategies are aligned, tasks and projects are prioritized, and that resources are appropriately allocated. Committee structures are often established to oversee these efforts. The committee structures (at multiple organization level) see that the work is completed in accordance with the healthcare company's objectives (Pourshahid, Amyot, Chen, Weiss, & Forster, 2007, May). Such individualized governance practices are driven by unique industry needs, industry structure, operations, and risk assessment.

Governance may also be addressed through a broader functional approach. COBIT (Control Objectives for Information and Information Related Technologies) has long been a foundational approach for information technology (IT) governance. It is also used to assess information systems functions and ascribe practitioner described normative ways to manage, administer and audit information systems. This governance framework is used by managers in managing and governing enterprise IT. An assessment of COBIT research found that COBIT is analyzed through multiple perspectives that focus on framework development and comparisons, or on specialized interest areas including security, risk management, systems development, effectiveness and internal control (often in the accounting domain). The breath of COBIT has increased over time to other areas of information systems (IS) related functions and operations. COBIT appears to continue to evolve. Suggestions have been made for expansion of COBIT IS governance in the areas of strategic alignment, COBIT adoption, implementation challenges, effectiveness, and framework tailoring for development (Mangalaraj, Singh, & Taneja, 2014).

A theoretical review of COBIT 5 qualitatively assessed the approach against: 1) Stakeholder Theory (SHT), 2) Principal Agent Theory (PAT), and 3) Technology Acceptance Model (TAM) (Devos, & Van de Ginste, 2015). The review focused on specifically selected IT components of COBIT because the COBIT framework is very broad and analyzes the complete IS function. The IT focus was selected for the review because of the theoretical and academic criticism of COBIT's lack of a theoretical basis, and its normative practitioner recommendations of how to manage, govern and audit IT in organizations.

The selected work focused on five COBIT 5 principles, five processes (APO13, BAI06, DSS05, MEA03 and EDM03) that address the area of IS security and four IT-related goals (IT01, IT07, IT10 and IT16). These principles and processes were chosen because they are centered on the IT related goals rather than the management and audit functions required within an organization (Devos, & Van de Ginste, 2015). The work found that COBIT offers a framework organizations can use to align IT and operational activities. COBIT 5 has 34 grouped IT control processes that are viewed as aligning the organizations IT activities when adhered to in a systematic fashion.

However, because RPA is not yet a standard IT solution/application, it is important to examine whether COBIT could be an adequate support framework to achieve the required alignment. COBIT could be an "answer" to the challenge the market is currently facing with respect to scaling RPA in that IT is usually insufficiently aligned with the business objectives. Each theory was used to develop testable propositions. The authors found that COBIT 5 holds theoretical supported claims. They concluded that the presence and contribution of a theoretical foundation is supported by the COBIT IT-related goals as compared to the processes (Devos, & Van de Ginste, 2015).

There appear to be various pragmatic governance approaches, but no strong or well examined theory of governance. The conclusion of "no real theory" exists for governance is supported by assessments of information systems research and literature in IT governance. A taxonomy of research encompassing the focus areas identified by the IT Governance Institute assessed strategic alignment, risk management, resource management, value delivery, and performance showed a lack of integration between these focus areas, and little about IT governance as a whole (Wilkin, & Chenhall, 2010). Wilkin and Chenhall emphasize this in concluding that there are several reasons for this molecular approach to IT governance. There has been a shift away from technologically focused research toward business-process/management issues including user interactions focusing on human collectives and interactions with IT (such as planning, strategy, resources, investment, value decision, methods, structures, and evaluations). Other work by Weill and Ross (2005) posited that a matrixed governance approach was utilized since no single best model for IT governance seemed to exist. The governance choice made by organizations seemed to depend upon decision-making related to the selection of strategic drivers, key metrics, available governance mechanisms, IT infrastructure, and IT principles.

Governance Models Research

Weill (2004) researched 250 companies that implemented various models of IT Governance. This work explained how top performers manage IT decisions to obtain higher performance. It reports that organizations can achieve value from IT by utilizing IT governance practices that vary. Successful IT governance models may be assigned according to various business archetypes including IT monarchy, federal, duopoly, feudal, and anarchy. These decision making approaches are used to govern decision rights granted for IT investment, architecture, principles, application choices and infrastructure. Firms leading on growth measures decentralize decision making by enabling business units to determine how to manage their IT. Firms that lead on profitability centralize decision rights and have decisions made by senior executives. IT governance is designed to reinforce the firm's objectives, governance of other assets, and reinforce desired behaviors and performance objectives.

A Governance Example – Heath Care

In healthcare, governance addresses complex and interrelated processes that have emerged over considerable time periods with shared and multilevel attributes. They seek to support collaboration among many diverse organizations over time periods while, at the same time, providing specific technical problem solutions to health organizations functions and departments (Paolo, Restifo, Gastaldi, and Corso, 2012). The two primary approaches discussed are internal and external governance required by different organizational objectives. Internal governance describes the set of policies, processes, decisions and rules that determine the way information systems are run, managed and developed. They note that low levels of formalization of these governance models affect the development of the information systems themselves. External governance is represented by the set of decisions that support information systems development adopted in health care organization through coordination with the other information systems used in the health care industry. There is value in obtaining data from other organizations in which the patients previously received treatments. Cooperation among the different organizations in the health care industry is important and external governance models seek to align the different interests in the sector. These governance mechanisms seek to develop connections among health care agents; promote industry integrated solutions with a positive social impact; and develop coordinating mechanisms that recombine, reuse, and recreate existing solutions while slowing amplifications and keeping the system under control (Paolo, et. al. 2012).

Governance Requirements – What about RPA?

A case presentation suggested for teaching governance by Kedziora (2021) proposed that several governance-related issues and decision points needed to be addressed in connection with any deployment of robotic process automation (RPA) on any somewhat large scale within a company. The proposed key issues and decisions are related to the RPA software's development and maintenance, RPAs' governance, and IT infrastructure. The learning objects were that students who worked through the case should be able to describe archetypal and hybrid governance modes for RPA, and evaluate the advantages and disadvantages (of RPA) while producing a solid infrastructure and effective software development and maintenance

2. ROBOTIC PROCESS Automation (RPA)

What is RPA?

Robotic Process Automation (RPA) has been discussed in popular management articles, information technology cases and research, and process literatures. Bloomberg (2018) describes this technology as one where ideally a piece of software performs the mundane tasks and employee interacts with some existing application. The employee, a human, does not have to click on buttons, input data copied from another source, or type data into fields in a form or other application.

The robotic program (bot) can perform these tasks, and with added artificial intelligence (AI) can perform cognitive tasks. These decisions are similar to the intelligent judgment decisions that humans have made previously. The attention and hype surrounding this technology is very great. The bots automate repetitive, rules-based processes previously (most often) executed by humans that are working at computer screens. The work is accomplished just as the human would perform a task of opening emails, reading attachments, filling in e-forms, and transcribing or re-keying data like an employee. RPA is very useful when the transactions are between older, legacy applications. The bots create a digital process flow that previously required manual steps. However, RPA workarounds may be required where changes to a user interface, the data, or the process are frequent or difficult to coordinate. RPAs may not function well if aspects of the legacy app, or interfaces change; or if task behavior cannot be executed as easily a human might. The bots interact with the user interface (UI) and can be error prone with changes. In some situations, APIs can perform more effectively than bots because they are more resilient and offer a better approach to automating interactions because they permit changes that are not disruptive (Bloomberg, 2018).

The Benefits of RPA

The pressure within an organization is to obtain the best of both worlds. The organization’s goals are to capture both the benefits of high task specialization and its enhanced task performance, and the RPA benefits of rapid and highly accurate task integration and performance. However, there are technical performance limitations (e.g., quality of the RPA technology, continued operation under conditions of changing systems, licensing, etc.) and cyber security risks, failure of proper execution sequences, and failure of operational controls that create new stresses on governance schemes previously used to manage systems that control and ensure the correct operation of specified functional systems. The stress placed on the governance processes is explored below by explaining the both the source of RPA benefits and value, and the RPA features that create the need for governance controls and support of the use of RPAs. These controls and support activities must be applied across differentiated systems that have not previously required such coordinated controls or oversight.

The benefits of RPA appear to derive from the impact it has on the design and implementation of organization processes when it is focused on areas where work has been divided into subcomponents. The division of work may be attributed to the task size, time, complexity, or human understanding limitations. The division promotes specialization and enhances task performance (speed, accuracy, learned behavior). The goal of the division of labor (specialization) is to improve organizational and management processes. These processes are the essential components of the assigned organizational work activities of employees, departments, and offices. When these activities are performed by bots (RPAs) the key outcomes are described with adjectives and adverbs that denote performance improvements in efficiency, speed, and accuracy. In essence, the organization is completing the required work or tasks more efficiently. The work was previously characterized as tedious and repetitive. However, with the RPA technology it is well executed, more accurate, and decision rules are consistently executed (Lacity, Willcocks, & Craig, 2015; Willcocks, Lacity, & Craig, 2017; Casey, 2020)

RPA and the Division of Labor

Adam Smith's book The Wealth of Nations published in 1776, clearly describes the specialization theory, better known as the division of labor. Smith argued that specialization could be performed by individuals, organizations, and nations. Smith historically argued that the division of labor will contribute to productivity increases under competitive conditions. This then contributes to product price reductions as markets and production expands. Smith theorized that production methods would then improve leading to the discovery of new ways of producing products and services with the cycle continuing until it is limited by the size of the market. As theorized, the division of labor and specialization of a worker’s tasks results from the processes of breaking large jobs into smaller jobs which can be performed more readily (Smith, 1937).

RPA is a modern technological resolution to the assembly of tasks that have been divided (for specialization). The work previously divided to take advantages of individual unique capabilities (Smith, 1937) must still be assembled to complete an entire task or goal. Managers and organizations must accumulate or integrate the divided work elements to accomplish the goals of producing the output desired by the customer and required by the business process.

This recombination of processes, and integration of sub-processes is an important part of delivering a service product or meeting an organization goal. Organizations have focused on integrating previously subdivided processes to offer more complex products and services and meet the requirements of highly complex product and service needs. Processes are viewed as frameworks containing steps in a sequence. The processes have many components, agents, and outcomes. A very complete discussion of the theory of group and organizational processes may be found in Mackenzie's Group and Organizational Processes, Volume I, II, III, IV (Mackenzie, 2015, 2016a, 2016b, 2020).

Can the highly specialized process steps be recombined and audited by RPA? In some (perhaps many) instances, the answer to this question is yes. But then one must ask about the impacts and durability of the results of the implemented RPA process.

This is the point where governance of RPA becomes important. Automated repetitive tasks are increasingly developed as RPAs, and adopted within organizations. They can be constructed (but perhaps not well) with limited IS skills, and development effort. RPA is incorporated into and between IT systems to enhance the value of a customer's experiences and reduce operating costs. The transformative opportunities can significantly alter processes in many areas such as banking where customers can more readily open accounts, and through insurance claims processes that streamline the steps that ensure insurers are able to readily identify fraudulent claims. But with RPA and process redesign, organizational risks can increase. Organizations that implement the RPAs may overlook the concerns traditionally addressed through governance compliance mechanisms, cybersecurity controls, and internal system audits. The requirements for cybersecurity, compliance and internal control must be incorporated into the systems applying RPA technologies whenever and wherever an organization is introducing RPA (Giesbers, 2020).

Vulnerabilities that apply to other systems or humans continue to be present in the new work processes incorporating RPAs. RPAs will stop working if they are compromised. The effects will result in process halting, work stoppage, and calls for steps to ensure continuity of operations. Further, the results of a compromised system may not be readily visible or quickly discovered. Data about employees or customers could be leaked on the dark web and made accessible to competitors. This action might not be noticed, or activate any immediate alarms. Consequentially, organizations may require time to realize a problem exists, discover that compromised bots have been incorrectly processing the data (such as billing incorrectly or paying a wrong party). RPA enhanced system risks are just as material and broad as the risks associated with an unadorned system or unaided human employee. The risks cross operational, financial, regulatory, and reputational categories (Giesbers, 2020).

Kosi (2019) discusses five cybersecurity concerns associated with the RPA technology. This work addresses the need for risk assessments in five areas and suggests possible security best practices. The first assessment area was RPA cybersecurity with attacks executed through abuse of privilege access via a compromised administrator account. Access to this ahis gives an attacker access to sensitive data. A former employee also could program the Bot to delete or alter data and stop processes prior to leaving an organization. The second risk was from the possible disclosure of sensitive data through an erroneously programmed bot that publishes confidential data that can is accessed by the public via the web, or steals and transmits intellectual property outside of the organization. Thirdly, the virtual machine environment presents risks where the bot runs. A security vulnerability in the virtual machine environment could permit an attacker to access the VM remotely and possibly access sensitive data, or permit a developer to program the bot to send/receive unencrypted sensitive data. Fourthly, a bot could contribute to a denial of service attack that enables one or many bots to utilize the virtual machine and make it unresponsive because all system resources are fully used. Finally, unplanned system upgrades or network maintenance for a virtual machine could instigate a loss in service or an outage.

These potential threats from RPA usage suggest there are some important considerations that must be addressed when governance is applied to RPAs.

The first general RPA consideration deals with data from a design, control, and security perspective. One must ask how internal control of data is maintained with regard to an RPA? The goal of control is to assure that processes in organizations provide a reasonable degree of certainty that the organization is accurately reporting, maintaining operations, and in compliance with laws and regulations. The goals are to identify and report variances from standards or expected results within a timely manner. This is accomplished by providing reliable information regarding financial and non-financial activity internally and externally; minimizing incorrect decisions and optimizing operational efficiency and effectiveness; and complying with the relevant laws and regulations to avoid legal conflicts.

Data management requires that deviations from the internal control goals of the organization be identified where raw data or information is not consistent with the underlying operational reality (appears unreliable); when inefficient and non-effective operations results in poor or incorrect decisions; and when failure to follow or obey laws and regulations (regarding data and its required handling processes) may result in legal conflicts (Giesbers, 2020).

A straightforward summary of the data controls required for RPAs is not significantly different from the data controls required of all effectively governed organizations.

They include data management policy, internal controls, change management, and configuration controls that address issues such as are the data:

> Designs complete, correct
> Definitions consistent
> Sequenced when appropriate with respect to timing, and age?
> Restorable and available for rollback
> Backed up for disaster recovery
> Protective of PII

A second major area of concern appears to address security. The questions that must be asked and addressed for RPA security concerns focus on the specialized cyber security risks introduced into the systems used by the organization with the development and production implementation of RPAs (Kosi, 2019).

The credentials required to access and execute RPAs provide an opportunity for cyber security intrusion and may open the systems interacting with the RPA tools to security threats and operational risks. These cyber "risks" and security vulnerabilities are associated with the credentials and access required by the RPA code. The RPA will be assigned privileges that grant the RPA access to read and write to information systems and data that reside within organizational systems and databases. This creates a "risk" from a cyber-security perspective under two different scenarios that are a function of the method of RPA bot operation.

There are two distinct operational categories. The first category is designated as the "attended" bots. These RPA bots are only able to execute their specified tasks when a defined user gives a command to perform a defined action, process, or to activate a specific process step.

Control of the attended bot is very simple under this scenario. A user must have credentials to perform a task that accesses a system or data. The bot can only execute using the credentials held by the user. Conceptually, the RPA bot "is" the user, or has privileges that the user possesses. It should be noted, that a strong governance mechanism would log and audit the actions the user performs as well as the tasks and actions the RPA bot performs more quickly.

The second condition is where the bot operates in an automated fashion based on a schedule, elapsed time, specific event, receipt of data or a request, etc. This is commonly described as an "unattended" RPA bot by the user community.

In this situation, the RPAs may simply fill in the task gaps—providing 24×7, cross-geography support for time-consuming, repetitive tasks that require completion to meet organizational goals. Designing and programming the automated bot is straightforward. First, a single manual process is used as the model for the design of the bot. It is the model used to create a business process flow. The bot would then be programmed to follow the defined flow. From there, any necessary rules, policies or exceptions that are used to complete that process are identified and added as decision rules, direction, and conditions that must be followed by the bot.

Exceptions would be segregated and assigned to humans to manage and resolve, and not executed by the bot. The robotic process is inserted into a production system (or possibly between production systems) and repeated according to the embedded pre-defined rules. Throughout this process, corrective actions can be made to bots to improve operations by recursively refining the process (and rules, new conditions, and actions) and maximizing operational efficiency of the un-attended RPA bot. The essential element that must be addressed is that the bot runs without direct supervision.

RPA and Privilege Connection

Analyses of the base use case for the unattended RPA bot must be made by security professionals charged with protecting the information systems and data of the organization. The IT security professionals' assessment will encompass a number of important factors (as with any information system) including assessment of the RPA connections to privileged credentials that can be used to access the data and systems of the organization.

Access credential are a large risk point, and simply put, a key factor that differentiates the unattended RPA bot from other programs and systems. The unattended bot offers a new attack vector. Organizations will need to ensure that all accounts are protected including the powerful, privileged administrative accounts within these RPA platforms.

RPAs (as described) are pieces of software that interact directly with business applications. The applications will permit (human) users with credentials to perform tasks. Since the RPA mirrors the human's actions, it will have "matching" or equivalent credentials and access entitlements. These access entitlements can introduce significant risks when/if the software bots automate and perform routine business processes across multiple systems. Therefore, it is important to minimize these risks by securing and carefully managing the RPA credentials.

In order to automate processes within a system environment, software bots need "power access" (or privileged access) to execute their tasks. Actions will include logging into a system(s) to access data, write data, or execute a trigger moving a process from step A to step B. A large amount of credentials must therefore be stored for execution, possibly within the RPA. RPA usage risks are derived from the attack vector presented by this situation. If the RPA password storage location is accessed by an attacker, these or other stolen credentials might be used to take control of the bots. The stolen credentials could also be used by the attacker to damage the systems, change data, etc., and (even worse) with RPA bots. Since the bots are automated (performing in an unattended fashion), the damage could be done on a very large scale, and to multiple systems. The magnitude of this risk is very great. Organizations that utilize multiple (hundreds or thousands) software bots which access numerous systems and perform multiple processes simultaneously must vigorously guard access credentials.

Pragmatically Locking Down RPA Credentials

The privileged account security challenges require careful credential management. The major characteristics of protecting credentials are found in the three steps listed below.

First, the organization can set up and manage a unique account for every system that is accessed by an RPA bot. The advantage of this approach is that the organization will not need to create domain or wider access credentials that would otherwise be leveraged by an RPA bot. Breaches or successful RPA based attacks will be limited to that specific system, and there will be no larger far reaching effect across other systems.

Secondly, bots can alternatively request and obtain their credentials from a centralized, encrypted location. The credentials would be obtained only when required by RPA tasks. In this situation, credentials for the RPA would be unique, and any hard-coded credentials would be retrieved for all bots.

There are some derivative advantages from the second pragmatic approach. A central credential storage location would be able to impose password policies for least privileges, enforce access limiting controls to only one job or system, force password rotation and uniqueness requirements, and suspend the passwords and credentials, if required. Finally, the administrator access to authorize privilege changes could be restricted to a single console (with no access to external networks). This would limit the possible attack vectors for attackers.

The second pragmatic solution is very powerful because no bots are permitted to execute under their own credentials, and there is no way for an attacker to use a bot or map the systems or applications of the environment for planning additional attacks. There are copies of the bot (stored in source control), and accessible if a user has developed a bot and leaves the organization. The bot can be maintained using this approach when upgrades or changes are necessary.

Pragmatically Addressing Operational Concerns

It is important to note that not all concerns are addressed by this approach. Bots could accidentally access sensitive data, over-write key information, and act as a "runaway" where a transaction that should have executed one time is performed many times. Thus, traditional safeguards including code registration processes, backups, restoration processes, logging and log reviews, and other operational metrics are all required with RPA development and use.

Robotic process automation follows a development and installation methodology as a software project. This context provides some difficulty in the testing areas similar to problems encountered when replacing an entire business process or outsource an activity. A “duplicate” production testing environment may not be available, and the RPA may not be able to encounter identical transactions that replicate all that may be processed over an extended period of time. Deploying the bots in the production environment introduces a higher degree of risk. Montero, Ramirez, and Enríquez (2019, May) designed an approach that generate a testing environment and a test case for an RPA project to address this risk.

The method devised has been prototyped and tested. It monitors the tasks and steps of the humans whose processes are targeted for the automation. A user interface log with the sequence of screen captures, mouse and key actions is verified. A test environment is then generated as a duplicate application that emulates operational environment with the use of the log information from the user interface. A control flow layer is then used to display screens based on the interface actions received. The test cases are finally used to validate that the RPA bot being tested correctly executes the user action stored in the user interface log.

3. WHERE AND WHY RPA TECHNOLGY GOVERNANCE MATTERS

How well do the governance control guidelines for the internal control aspects organizations apply to RPAs, and ensure that RPAs are operating in a secure and compliant way?

The governance models and controls have some direct relevance to the RPA processes described. For example, organizations manage data through data governance processes that function across an entire organization. Data governance rules are formal processes and policies that are designed to ensure that data are controlled in a well-defined manner. Rules are set for creating, collecting, handling, and securing information. Data must be transparent, and useful for the organization members with authorized access. Strategies for accomplishing this include requiring control and monitoring processes that apply to all processes and systems. The processes address storage, maintenance, exchanges, and synchronization requirements that make data consistent, accurate, and timely (White, Newman, Logan, & Radcliffe, 2006). The data may include: core data (identification, customer, product, employee, vendor, etc.) used to categorize and aggregate and transactional data documenting activities from operational systems that describe activities, or transactions.

The authority and control over the management of data is considered to be data governance by Abraham, Schneider, and Vom Brocke (2019). In their assessment of 145 research papers (published from 2001-2019) they identify the major building blocks of data governance and decompose them along six dimensions. The governance building blocks included: cross-functional efforts, a formal structured framework, a strategic enterprise asset, specifies decision rights and accountabilities regarding decision-making about an organization’s data; data governance developed data policies, standards, and procedures consistent with the organization’s strategy to promote desirable behavior in the use of data; and compliance monitoring. They also note that data governance refers to what decisions must be made and who makes those decisions, whereas data management is about making those decisions as part of the day-to-day execution of data governance policies.

Research has indicated the data governance is a contributor to success systems and productivity. Henriques, Pereira, Bianchi, Almeida, and da Silva, M. M. (2020) assessed the governance concerns for the Internet of things (IoT) and its impact upon organizational IT strategy alignment and infrastructures with regard to the organizations’ business objectives. The COBIT enabler categories seek to facilitate the implementation, identification, and management of IT by providing governance enablers that assist managers in improving IoT implementation. The findings in this work indicate that data privacy, data protection, and data analysis are currently the most relevant enablers. During the IT implementation these enablers increase the solution’s efficiency and enhance data credibility.

However, the example governance framework discussed (COBIT) makes no direct mention of RPA or the other threats hypothesized from an operational perspective.

RPA and Governance Models

No governance models specifically address governance for RPA, at this time.

Issues and Concerns with the RPA Technology

RPA governance was assessed by Boekhoudt (2019) to determine how well the functional COBIT approach could be applied to meet the governance requirements for audit control. The assessment concluded that COBIT was adequate as a framework that could be applied to align IT and RPAs business requirements. However, there may not be (at that time) sufficient knowledge and expertise with RPAs to apply COBIT. The work concluded that RPA is an innovative and emerging technology with new and specific risks that should be completely assessed when applying COBIT. Several specific areas of assessment were identified in the research including: systemic error propagation attributed to a missed data or process change, design errors, and unforeseen exceptions in the process; bot access and credentialing; monitoring the execution of locally run bots on laptops and decentralized distribution throughout the whole organization; and setting coding standards for reliability and maintenance. This work notes that some vendors may establish design standards that aid in the technical implementation processes that include: maintaining flexibility by storing environment settings in external configuration files; security by saving credentials externally and not in the design; maintaining readability with meaningful names and comments; utilizing structure and development standards to effectively change bots; and embedded exception handling and error reporting.

Giesbers (2020, p. 189) assessed how to control RPA bots in an organizations and avoid security and compliance risks. This work performed assessments of the RPA theoretical risk and control framework. It concludes that "…there are some small differences between RPA and 'general' IT. But overall RPA is not that different from 'general' IT…" It posits that it is possible to leverage a large part of the already existing controls to manage RPAs. The control topics that require specialized RPA attention according to this study were: security roles and responsibilities, policies and policy reviews, enterprise controls and risk control framework, continuity framework, security education awareness and training, secure systems engineering principles, security testing, quality assurance, secure login during run-time, and ownership of RPA assets (Giesbers, 2020, p. 182-184).

4. RPA FAILURES

This paper has described many potential avenues for RPA "failures" and sought to explore the issues and stresses these potential failures pose for organization-wide RPA governance. A logical question comes to mind – have the RPAs failed (as they might), and are the hypothesized difficulties documented in the practitioner literature or academic research? None of the published works cited in this paper or other uncited papers addressing the uses and benefits of RPAs identify or discuss any instances of "failures," compromised systems, or operational issues. This lack of direct evidence or cases of RPA related or instigated failures may be a function or the new and unique nature of this technology, or attributed to attackers' failure to "recognize" the potential of a new attack vector. Regardless of the reason, the articles that hypothesized about the possibilities of RPA failures, security intrusions, and operational issues or damage did not provide direct references to specific occurrences or list organizations that experienced these types of negative outcome.

However, there are some discussions of the failure of RPA projects in the literature reviewed. Lamberton, Gillard, and Kaczmarskyj (2016) discussed concerning RPA statistics based upon consulting studies which demonstrate that initial RPA projects fail 30% to 50% of the time. The source document indicates that the failures cited are not related to RPA misuse or mistakes with regard to security or other operational issues. The failures listed in Table 1 were attributed to a variety of leadership, business, project and organizational issues.

Table 1 Types of RPA Failures

Description of Failure
Not considering RPA as business led, as opposed to IT led.
Not having an RPA business case and postponing planning until after proof-of-concepts (POCs) or pilots
Underestimating what happens after processes have been automated
Treating robotics as a series of automations vs. an end to end change program.
Targeting RPA at the wrong processes.
Applying traditional delivery methodologies
Automating too much of a process or not optimizing for RPA
Forgetting about IT infrastructure

5. CONCLUSIONS AND RECOMMENDATIONS

As more and newer technologies evolve, pressures will increase on organizations to utilize and adopt the technologies and achieve immediate ROI. Robotic process automation (RPA) is a relatively new information technology tool that is receiving attention and invoking adoption pressures. However, organizations may be reluctant to adopt new technologies because of fears of possible risks of failure and capital cost losses (opportunity losses) from direct fiascos and consequential damages. These decision making fears are real for managers, and true impedances to adoption (but not necessarily supported by case data or by documented bot technology failures). One can readily recall failures that have previously occurred with technologies such as Segway, Google glasses, electronic voting, CRISPR babies, and data trafficking.

IT implementations are more likely to succeed (but never fully assured of success) when system selection, development, operational frameworks and models of performance are followed. The COBIT IT management and governance framework is applied to aid in the development, organization and implementation of IT. Today this framework addresses information, communication, risk management, information governance, and collaborative and changing technology.

This paper assesses research and literature addressing RPA and COBIT (as one governance technology). The features and differences of RPA and other IT systems and implementations were not determined to be enormously different or demanding of a new governance framework. Elaboration and tailoring are suggested as an appropriate approach to provide assurance to managers and RPA users that this tool is not a significant new or unknown risk to enterprise use.

However, it is recommended that the using or adopting organizations pay specific attention to the data controls and management and security features of the RPA technology. The recommendations are that requirements be established and systems using RPAs monitored for: explicit segregation of duties: digital identity and access management; data encryption (including credentials); maintain policies for data classification, data retention, data storage, and data location; monitoring of logs and regular auditing; and scanning of all bot programs for vulnerabilities prior to promotion into the production environment.

It is also recommended that organizations recognize that access credential present a key risk factor and attack vector for unattended RPA bot. Organizations should ensure that all accounts including privileged administrative accounts are protected when employing RPA.

6. ACKNOWLEDGEMENTS

The contributions, criticisms, and comments of the reviews are greatly appreciated. All errors and omission remain the sole responsibility of the author.

7. REFERENCES

Abraham, R., Schneider, J., & Vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. International Journal of Information Management, 49, 424-438.

Bloomberg, J. (2018). Why You Should Think Twice About Robotic Process Automation. Haettu, 26, 2019.

Boekhoudt, S. Aligning IT with RPA business requirements through COBIT. RESEARCH IN IT-AUDITING AM, 215.

Casey, K. (July, 2020). 5 ways to define RPA in plain English. The Enterprisers Project. Retrieved March 18, 2021 from https://enterprisersproject.com/article/2019/5/rpa-robotic-process-automation-how-explain

Devos, J., & Van de Ginste, K. (2015). Towards a theoretical foundation of IT governance: the COBIT 5 case. In ECIME (Vol. 18, No. 2, pp. 95-103). Academic Publishing Limited.

Giesbers, S. (2020). Robotic process automation and internal control: a guideline. Research in IT-Auditing: a Multidisciplinary view Edition, 171.

Henriques, D., Pereira, R., Bianchi, I. S., Almeida, R., & da Silva, M. M. (2020). How IT Governance can assist IoT project implementation. International Journal of Information Systems and Project Management, 8(3), 25-45.

Kedziora, D., & Penttinen, E. (2021). Governance models for robotic process automation: The case of Nordea Bank. Journal of Information Technology Teaching Cases, 11(1), 20-29.

Kosi, F. (2019). Robotic process automation (rpa) and security. Master’s thesis, Mercy College.

Lacity, M., Willcocks, L. P., & Craig, A. (2015). The IT Function and Robotic Process Automation.

Lamberton, C., Gillard, A., & Kaczmarskyj, G. (2016). Get ready for robots-Why planning makes the difference between success and disappointment. United Kingdom: EYGM Limited.

Mackenzie, K.D. (2015). Group and organizational processes, volume I: The quest to discover their essence. Saarbrücken, Deutschland / Germany: Lambert Academic Publishing.

Mackenzie, K.D. (2016a). Group and organizational processes, volume II: Organizational applications. Saarbrücken, Deutschland / Germany: Lambert Academic Publishing.

Mackenzie, K.D. (2016b). Group and organizational processes, volume III: Organizational leadership. Saarbrücken, Deutschland / Germany: Lambert Academic Publishing.

Mackenzie, K.D. (2020). Group and organizational processes, volume IV: A better science for managing. Mauritius: Lambert Academic Publishing.

Mangalaraj, G., Singh, A., & Taneja, A. (2014). IT governance frameworks and COBIT-a literature review.

Montero, J. C., Ramirez, A. J., & Enríquez, J. G. (2019, May). Towards a method for automated testing in robotic process automation projects. In 2019 IEEE/ACM 14th International Workshop on Automation of Software Test (AST) (pp. 42-47). IEEE.

Paolo Locatelli, P., Restifo, N., Gastaldi, L., & Corso, M. (2012). Health care information systems: architectural models and governance, in Kalloniatis, C. (Ed.). Innovative Information Systems Modelling Techniques. BoD–Books on Demand.

Pourshahid, A., Amyot, D., Chen, P., Weiss, M., & Forster, A. J. (2007, May). Business Process Monitoring and Alignment: An Approach Based on the User Requirements Notation and Business Intelligence Tools. In WER (pp. 80-91).

Smith, A. (1937). The wealth of nations. Modern Library Classics. New York, 423.

Wang, P., & Johnson, C. (2018). Cybersecurity incident handling: a case study of the Equifax data breach. Issues in Information Systems, 19(3).

Weill, P., & Ross, J. (2005). A matrixed approach to designing IT governance. MIT Sloan management review, 46(2), 26.

White, A., Newman, D., Logan, D., & Radcliffe, J. (2006). Mastering master data management. Gartner Group, Stamford.

Wilkin, C. L., & Chenhall, R. H. (2010). A review of IT governance: A taxonomy to inform accounting information systems. Journal of Information Systems, 24(2), 107-146.

Willcocks, L., Lacity, M., & Craig, A. (2017). Robotic process automation: strategic transformation lever for global business services? Journal of Information Technology Teaching Cases (pp. 1-12). ISSN 2043-8869