Auditing an RPA-Enabled Accounting Information System

Deniz Appelbaum & Stephen Kozlowski

47th WCARS Symposium
Newark, NJ
November 8 & 9, 2019

Introduction

- Robotic Process Automation (RPA):
  - Provides the tools to create software robots that can automate business processes.
  - The robots can interact with any system or application the same way a human does (Automation Anywhere, 2019).
- The Institute of Electrical and Electronics Engineers (IEEE) Standards Association provides a much more formal definition of Robotic Process Automation (RPA):
  - ''A preconfigured software instance that uses business rules and predefined 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'' (IEEE Corporate Advisory Group 2017) (Moffitt, Rosario, & Vasarhelyi, 2018).
- When described in terms of service automation, software robots are engaged to perform repetitive and routine service tasks that have been previously performed by humans, allowing humans to focus on more unstructured and interesting tasks (Lacity & Willcocks, 2017).

Introduction

- Robotic process automation (RPA) provides the tools and platforms that deal with:
  - Structured data
  - Rules-based processes
  - Deterministic outcomes
- There is a wide range of service tasks suitable for RPA.
- Organizations seeking to automate services have multiple sourcing options:
  - Insourcing: buying service automation software licenses directly from a service automation provider.
  - Insourcing and consulting: buying licenses directly from a service automation provider and engage a consulting firm for services and configuration.
  - Outsourcing with a traditional business process outsourcing (BPO) provider: buying service automation as part of an integrated service delivered by a traditional BPO provider.
  - Outsourcing with a new provider: buying service automation from a new outsourcing provider that specializes in service automation.
  - Cloud sourcing: buying service automation as a cloud service. (Lacity & Willcocks, 2017)

Introduction

- RPA possesses unique characteristics that set it apart from other automation paradigms contained in:
  - Business process automation
  - Business process reengineering
  - Business process management systems
- RPA robots conduct work the same way that humans do, through the software presentation layer.
  - Logins, emails, analyses, report building, data entry, and other functions are still completed (Moffitt et al., 2018)
- Although the scope of RPA-appropriate tasks and processes is increasing, there are certain attributes that are helpful in identifying them (Lacity, Willcocks, and Craig 2015):
  - Well-defined processes are more automatable. Because robots currently still need precise instructions in order to successfully complete tasks, tasks with significant ambiguity are not typically candidates for automation.
  - High volume, repeated tasks can benefit more from automation. Tasks associated with payroll, accounts payable, and accounts receivable are often mundane and recurring, making them good candidates.
  - Mature tasks should be targeted. They have more predictable outcomes and the costs are known. Automating these types of tasks is less risky.

Introduction

- For audit automation to add value and improve audit quality, it is important to evaluate the reliability of the data:
  - Data validation checks, such as ensuring proper segregation of duties and tests of application controls, can help auditors assess the validity of data contained within digital reports that are to be used for RPA-based audit testing.
  - Reliable electronic audit evidence would be the first stage toward data standardization.
  - Data standardization can then be accomplished by selecting audit-related data fields from reports and importing them into an ADS for a particular audit area.
  - As the data that are transferred from one source to a standardized template can suffer from data corruption, audit firms should also consider data validation checks to reconcile data from the original reports to the data per the ADS.
- This research will investigate and document the audit-related issues that arise due to the incorporation of RPA tools in a typical Accounting Information System.
- We will identify RPA-specific issues that may impact the audit process with respect to specific accounting-related business processes, the RPA tools being utilized, and the varied types of data and data sources that drive the process.

Proposed Audit Processes

- This research will focus on a selected number of accounting processes that may be best suited to RPA. Such examples may include:
  - Customer invoice generation and processing
  - Vendor invoice verification, recording, and processing
  - Customer payment receipt verification, recording, and processing
  - Vendor payment generation and processing
  - Financial statement, general ledger, and other accounting reporting creation and distribution
  - Account reconciliations

Assets of RPA

- Firms that seek to use RPA tools should consider how these tools will be validated and deemed reliable. (Appelbaum et al. 2017)
- Firms should review the settings of the RPA software and run data simulations that can enable them to observe the inputs and the expected outputs of the RPA software.
- This research will investigate the following questions:
  - How frequently should RPA software validation occur (Moffitt et al 2018):
    - annually,
    - quarterly,
    - in anticipation of the annual audit,
    - or on a continuous basis?
  - How much control does the firm have over the RPA tool (Moffitt et al 2018)?
  - Is the tool built on a third-party platform?
    - Did this third-party company receive a SOC report?
  - Is the tool built in-house?
  - Did the firm clearly identify the tasks for the RPA?
  - Did the firm flow-chart the processes?

Assets of RPA

- This research will investigate the following questions: (continued):
  - Does the RPA match the flow-charted manual processes?
  - Is the RPA tool maintained in-house or by a third party?
  - Can the firm update the RPA tool or is this done externally?
  - Does the firm maintain an updated firewall around all steps of the RPA process?
    - Does the firm leave its own database at any time?
    - Does this process occur in the cloud?
    - Does the firm have control of this cloud environment?

RPA Data

- It is important to evaluate the reliability of the data.
  - Data validation checks, such as ensuring proper segregation of duties and tests of application controls, can help assess the validity of data contained within digital reports that are to be used for RPA-based audit testing.
  - Reconcile the data from the original data source through all intermediate steps to the final report is key.
  - Questions may evolve as follows:
    - What types of data are being processed (Moffitt et al 2018)?
      - Internal and/or quantitative?
      - Internal and/or external text? Machine readable or PDF?
      - Internal and/or external other media (video, audio, pictures, sensor readings)?
    - Is the data format consistent (Moffitt et al 2018)?
    - Is the data source reliable (Moffitt et al 2018, Appelbaum 2016)?
    - Can the auditor vouch for the provenance of the data (Appelbaum 2016)?

RPA Audit Methodology

- This research will utilize the guidelines established by NIST for assessing the risks of technology applications.
- In order to build a reliable framework based on established principles, we reference the concepts and terminology adapted from the NIST's Special Publication 800-30 (NIST 2012) for an evaluation of inherent risk.
- According to NIST (2012), an inherent risk assessment should identify:
  - Threats to organizations (i.e., operations, assets, or individuals);
  - Vulnerabilities internal and external to organizations;
  - The harm (i.e., adverse impact) that may occur given the potential for threats exploiting vulnerabilities; and
  - The likelihood that harm will occur.
- This research incorporates each of the above elements and an analysis of those elements, along with example internal control activities and procedures for addressing their associated inherent risks.
- We designate a low, moderate, or high level of likelihood to each inherent risk of a process. The likelihood of inherent risk is dependent on the characteristics of the process in question.
  - It may vary from organization to organization based on complexity and purpose, and on the extent of reliance that the organization places on the relevant process.

RPA Audit Methodology

- RPA inherent risks are those that are present, prior to implementation of controls, in relation to the use of RPA across any relevant organization processes. Inherent Risks for RPA could be:
  - Hacking: hacks could occur at any point of the process, including data input. Such hacks could snoop, copy, or alter transactions.
    - For example, an RPA Bot that has been trained to sort, open, and process emails will need to know how to identify a phishing email. A phishing email may or may not present itself with very minor grammatical or design errors which may be hard for a bot to detect and the return address may even appear legitimate.
  - Data Quality: Many of the data quality issues have been mentioned earlier and comprise of data origin, data processing, data consistency, data type, and frequency.
  - Process Changes: Process changes that impact the RPA task may cause it to abort or process an error.
    - This may occur as a format change with incoming documentation, a new data format, or a new source location, to name but a few of the ways an RPA task could be affected. Also, the RPA should be programmed to reflect any internal process changes.
  - Software Failures: These failures might occur with the RPA software itself and/or with platform or software failures of components that the RPA interacts with.
  - Staff Competency: Staff should be familiar with how the RPA code is generated and make efforts at maintaining ongoing training.
    - Staff might become too knowledgeable and be able to alter the code for fraudulent gain.
  - Authorization: Many processes require authorization to proceed at various stages. The RPA should be carefully programmed to authenticate the authorization stage and pause the process if faced with any conflicting or questionable input.
  - Fraud & Collusion: An RPA process could be used for fraudulent purposes if users and recipients are in collusion.

RPA Audit Methodology

- **RPA Threats and Vulnerabilities:**
  - Threats and vulnerabilities are how any inherent risk may present itself.
  - Examples of specific threats and vulnerabilities have been linked directly to the processes being evaluated.
  - These are identified for each inherent risk.
    - Threats are labeled as high, moderate, low, and none.
    - Vulnerabilities are labeled as high, moderate, low, or none.
- **RPA Likelihood and Impact:**
  - Likelihood and impact are expressed as a highly generalized estimate, related to specific threats or vulnerabilities.
  - Overall, this is a difficult component to estimate given considerations for human behavior and does not represent all possible company or individual circumstances.
  - This is the largest judgement-based component of this framework.
  - The likelihood and impact of inherent risk issues are evaluated for each firm that uses RPA.
    - Likelihood is labeled as high, moderate, low, and none as Impact.

RPA Audit Methodology

- **RPA Internal Control Activities and Procedures:**
  - These are suggested specific activities, procedures, and protections that potentially mitigate the outlined threats and vulnerabilities tied to RPA inherent risks.
  - These internal controls are anticipated to mitigate the threats stemming from the inherent risks.
  - What follows is a presentation of the inherent RPA risks, threats, vulnerabilities, likelihood, impact, and IC activities for each type of accounting process that will likely be processed with RPA

RPA Audit Methodology

Transaction	Inherent risks	Threats & Vulnerabilities	Likelihood	Impact	Expected Internal Control Procedures
Customer invoice generation and processing	1-hacking into invoice, pricing, customer, and inventory item data	High threat, moderate vulnerability	Moderate	High	-Access controls -monitoring of RPA process -monitoring of RPA results
	2-data quality	Moderate threat, high vulnerability	High	Severe	-Data validation checks -Segregation of duties -Application controls
	3-process changes	Low threat, moderate vulnerability	Low	High	-Periodically check the RPA -Alert response -Access controls
	4-software failures	Moderate threat, moderate vulnerability	Moderate	High	-Periodic setting reviews -Management approval of changes -Testing of changes -User approval of changes
	5-staff competency	Low threat, low vulnerability	Low	Moderate	-Staff training
	6-authorization	Low threat, moderate vulnerability	Low	Moderate	-Access controls
	7-fraud & collusion	Moderate threat, high vulnerability	Low	High	-Segregation of duties -Supervision

RPA Audit Methodology

Transaction	Inherent risks	Threats & Vulnerabilities	Likelihood	Impact	Expected Internal Control Procedures
Vendor invoice verification, recording, and processing	1-hacking into invoice, pricing, vendor, and inventory item data	High threat, moderate vulnerability	Moderate	High	-Access controls
	2-data quality	Moderate threat, high vulnerability	High	Severe	-Data validation checks -Segregation of duties -Application controls
	3-process changes	Low threat, moderate vulnerability	Low	High	-Periodically check the RPA -Alert response -Access controls
	4-software failures	Moderate threat, moderate vulnerability	Moderate	High	-Periodic setting reviews -Management approval of changes -Testing of changes -User approval of changes
	5-staff competency	Low threat, low vulnerability	Low	Moderate	-Staff training
	6-authorization	Low threat, moderate vulnerability	Low	Moderate	-Access controls
	7-fraud & collusion	Low threat, high vulnerability	Low	High	-Segregation of duties -Supervision

RPA Audit Methodology

Transaction	Inherent risks	Threats & Vulnerabilities	Likelihood	Impact	Expected Internal Control Procedures
Customer payment receipt verification, recording, and processing	1-hacking into customer, customer banking, and payment data	High threat, high vulnerability	Moderate	High	-Access controls
	2-data quality	High threat, high vulnerability	High	Severe	-Data validation checks -Segregation of duties -Application controls
	3-process changes	Low threat, moderate vulnerability	Low	High	-Periodically check the RPA -alert response
	4-software failures	Moderate threat, moderate vulnerability	Moderate	High	-Periodic setting reviews
	5-staff competency	Low threat, Low vulnerability	Low	Moderate	-Staff training
	6-authorization	Low threat, moderate vulnerability	Low	Moderate	-Access controls
	7-fraud & collusion	High threat, high vulnerability	Moderate	High	-Segregation of duties -Supervision

RPA Audit Methodology

Transaction	Inherent risks	Threats & Vulnerabilities	Likelihood	Impact	Expected Internal Control Procedures
Vendor payment generation and processing	1-hacking into vendor, invoice, firm's banking information	High threat, high vulnerability	Moderate	High	-Access controls
	2-data quality	High threat, high vulnerability	High	Severe	-Data validation checks -Segregation of duties -Application controls
	3-process changes	Low threat, moderate vulnerability	Low	High	-Periodically check the RPA -alert response
	4-software failures	Moderate threat, moderate vulnerability	Moderate	High	-Periodic setting reviews
	5-staff competency	Low threat, moderate vulnerability	Low	Moderate	-Staff training
	6-authorization	Moderate threat, high vulnerability	Low	Moderate	-Access controls
	7-fraud & collusion	High threat, high vulnerability	High	High	-Segregation of duties -Supervision

RPA Audit Methodology

Transaction	Inherent risks	Threats & Vulnerabilities	Likelihood	Impact	Expected Internal Control Procedures
Financial statement, general ledger, and other accounting reporting creation and distribution	1-hacking into firm's AIS, accounting data	High threat, moderate vulnerability	Moderate	High	-Access controls
	2-data quality	Moderate threat, high vulnerability	Moderate	Severe	-Data validation checks -Segregation of duties -Application controls
	3-process changes	Low threat, low vulnerability	Low	High	-Periodically check the RPA -alert response
	4-software failures	Moderate threat, low vulnerability	Moderate	High	-Periodic setting reviews
	5-staff competency	Low threat, Low vulnerability	Low	Moderate	-Staff training
	6-authorization	Low threat, moderate vulnerability	Low	Moderate	-Access controls
	7-fraud & collusion	Low threat, moderate vulnerability	Low	Moderate	-Segregation of duties -Supervision

RPA Audit Methodology

Transaction	Inherent risks	Threats & Vulnerabilities	Likelihood	Impact	Expected Internal Control Procedures
Account reconciliations	1-hacking into externally-sourced data to support the process (for example, bank statement data)	High threat, moderate vulnerability	Moderate	High	-Access controls
	2-data quality	Moderate threat, moderate vulnerability	Moderate	Severe	-Data validation checks -Segregation of duties -Application controls
	3-process changes	Low threat, low vulnerability	Low	High	-Periodically check the RPA -alert response
	4-software failures	Moderate threat, low vulnerability	Moderate	High	-Periodic setting reviews
	5-staff competency	Low threat, Low vulnerability	Low	Moderate	-Staff training
	6-authorization	Low threat, moderate vulnerability	Low	Moderate	-Access controls
	7-fraud & collusion	Low threat, moderate vulnerability	Low	Moderate	-Segregation of duties -Supervision

Discussion

- The incorporation of additional tests and audit routines in an RPA-enabled AIS should not dramatically impact the audit process.
- The scope of work will increase due to the need to audit the imbedded RPA functionality. The additional audit tests and routines can, to an extent, mirror those in place for auditing other IT systems.
- The expected internal control procedures, as noted in tables, should be similar to those for other IT systems.
- It is expected that RPA tasks, acting in an expanded fashion from those automated tasks presently incorporated in IT systems, will include activities such as accessing information from an external, internet website, as compared to IT automation tasks that function solely with the confines of the AIS and related DBMS.
- More sophisticated audit tests will need to be developed to adequately test such functionality.
  - Testing the interface, or hand-off, of information from RPA to the AIS will require additional sophistication as the information may include a variety of data types where translation errors may occur in the interface.

Conclusion

- Even though RPA is anticipated to reduce the time that an auditor spends on highly repetitive, mundane, and error-prone tasks, the auditor cannot relax her professional skepticism.
- The auditor should constantly test as to whether the RPA is truly reliable, creating perfect audit trails, and reducing mistakes, as its proponents claim (Moffitt et al 2018).
- Auditors should not "drink the Kool-Aid" and should instead review the inherent risks of the RPA processes and evaluate their threats, vulnerabilities, likelihood, impact, and controls.
  - Whether the auditor is examining a client's RPA or her own RPA, the process remains the same.
- As technology becomes more and more intertwined with human processes with humans relinquishing actions of certain tasks to RPA bots, the auditor will be required to evaluate these controls more frequently and perhaps even on a continual basis.
- The time may be arriving where technology platforms and processes should be accompanied with a SOC-type report.
  - This would provide an independent and thorough analysis of many aspects of the software or technology that are not available for the typical IT auditor and would allow her to fine tune her audit process.
- At some point standard setters will need to provide guidance as to the reliability of an RPA-derived source of audit evidence.
  - Would the audit evidence generated by an auditor's RPA bot be considered to be as reliable as evidence generated by the auditor herself?
- These are but a few points that the audit profession will need to consider while undertaking the assurance examination of an RPA-enabled AIS.