FEATURE

Inherent Risk in Adopting RPA and Opportunities for Internal Audit Departments

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2oGSsIz

Many organizations are rapidly moving to implement robotic process automation (RPA) because it helps leverage multiple fronts, including cost advantage, workforce optimization, quality improvements, flexible and dynamic execution, speed, and agility.

As per industry estimates, "45% of workforce tasks can be automated, which could save an estimated [US]$2 trillion in global workforce costs."[1] As RPA and its use expand, internal audit cannot help but face formerly human-controlled processes that are now performed robotically. Within the next few years, internal audit is increasingly likely to encounter RPA in routine audit engagements.

This opens a new vista of challenges and opportunities for internal auditors as they start deciphering the inherent risk posed by a new technology that has altered processes to accommodate that same technology and new emerging risk.

There are opportunities that await internal audit (IA) while organizations race toward RPA implementation:

- Since IA interfaces with several departments and audits several processes within an organization, it can be helpful to identify opportunities to embed automation-enabled control activities within the business processes and departments.
- Most importantly, IA "can help to integrate governance, risk, and controls considerations throughout the automation program life cycle as an organization establishes and implements its program."[2]
- IA can also employ RPA innovations to increase the efficiency and effectiveness of its own department. These innovations can include the following:[3]
  - Leverage RPA to test the full population rather than limited sample testing
  - Increase IA capability by boosting the coverage and frequency of testing across the audit universe
  - Expand the audit scope for individual audits
  - Employ RPA to perform routine administrative activities and, thereby, improve efficiency of planning, testing and reporting activities, creating more time for critical-thinking activities
  - Enhance quality aspects of audits and monitor consistency of internal audit processes
  - Manage and enhance IA team's utilization working with a globally diverse team

Inherent Risk of RPA

RPA implementation often includes process redesign, which introduces new risk to organizations. Therefore, internal audit should consider specific risk factors when evaluating RPA pilots or implementations.

Misconfigured Human System Integration

In certain scenarios, RPA implementation can be tricky, and organizations need to be extra careful to ensure that bot access does not automatically initiate other types of rights for services. In one scenario, due to a lack of proper human system integration and monitoring, the creation of an employee ID for a bot also triggered the allocation of office seating and the purchase and delivery of cell phones and ID cards.

Gaurav Priyadarshi, CISA, BS 25999 LI, ISO 27001 LA, ITIL v3, CSA Star Certified Auditor
Is a senior auditor at Metlife GOSC and has more than a decade of global experience in audit and information security consulting. Priyadarshi is a technology evangelist and a follower of trending audit concepts. He can be reached at gpriyadarshi@gmail.com.

Overdone Automation
RPA is a new tool with low implementation costs and quick turnaround time, but there can be scenarios where organizations run the risk of implementing the tool in processes where manual modes or traditional tools work more efficiently.

Tough Change Management
RPA implementation requires considerable effort to manage the changes brought to the process and job content of employees. Mismanaged change management across the organization can result in the failure of the automation efforts.

Implementation Gaps and Mismanagement
RPA implementation comes with several complexities in the form of process redesign, operation procedure changes, administrative challenges, new monitoring processes and possible team restructuring. It is imperative for a successful rollout that a robust governance structure with clearly defined roles and responsibilities is defined and established.

> “RPA IMPLEMENTATION OFTEN INCLUDES PROCESS REDESIGN, WHICH INTRODUCES NEW RISK TO ORGANIZATIONS.”

Misaligned Vendors/Third Parties
One benefit of RPA is that it requires a short time period to implement; however, this can result in a scenario in which other stakeholders such as vendors and third parties are not able to keep pace or are not prepared for the change in the process brought by RPA. Organizations run the risk of bringing in RPA in silos without factoring in how vendors and third parties will cope with it. RPA necessitates a well-designed integration of vendors/third parties in the planning process of its implementation.

Violation of Corporate Security Policy
RPA exposes organizations to new types of cybersecurity threats as more and more processes

become automated, thereby posing challenges to existing IT security protocols and, thus, increasing IT risk.

Hacking Threats/Cybersecurity Risk
Introducing a new technology to an organization always comes with certain vulnerabilities that can be exploited by hackers. For example, automated solutions or bots may not have the ability/functionality to identify malware, thereby increasing the threat and providing opportunity to hackers.

Lack of Security Standardization for RPA
As of now, there is no security standard/guideline among RPA vendors. As such, there is no security standardization.

Opportunities for Internal Audit in RPA

IA can leverage the previously mentioned challenges in RPA implementation and use them as opportunities to assist the organization in several areas.

Creating a Robust Governance Structure to Assimilate Changes Brought by RPA
As with the introduction of any groundbreaking technology, RPA also brings along the challenge of governance issues. Thus, it is imperative that organizations make changes to the existing governance structure and related policies to assimilate the changes brought by RPA. IA can play a vital role in this to ensure that a proper governance

Enjoying this article?

- Read *Audit Outlook: Intelligent Automation. www.isaca.org/audit-outlook-intelligent-automation*
- Learn more about, discuss and collaborate on emerging technology in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

structure is created and implemented and that roles and responsibilities are appropriately defined for developing and maintaining governance controls. "IA can also take the responsibility to define the approach that will help determine which processes are appropriate for RPA, how RPA is implemented and how the processes are maintained."[4]

Addition of New Controls and Their Review
The introduction of RPA in an organization will often lead to changes, including process re-engineering. IA must ensure that a new control is defined and new risk factors identified. Then, IA can audit them to provide assurance to management.

Business Continuity Planning (BCP)
Technologies such as RPA are disruptive, but they are also prone to business-disruptive scenarios such as disasters. IA can thus review and give assurance to the business that the newly automated systems have backup plans for continuing critical operations in a disaster event that may lead to RPA systems going down accidentally or on purpose.[5]

Exception Management
RPA can bring about new complexity to the organization. For example, it can increase the volume of transactions processed, which may greatly increase the number of process exceptions. IA can be tasked with auditing these exceptions and making sure that there is a clear process in place to effectively manage these exceptions.

Conclusion

RPA is here to stay, will grow exponentially and will make rapid headway into organizations. The role of internal audit departments will increase as organizations embrace new risk scenarios that come with adoption of this technology. Internal audit departments can leverage this as an opportunity to define and provide assurance around governance, controls review, exception management and business continuity, and thus support the automation across the organization.

Endnotes

1 PricewaterhouseCoopers, "Robotic Process Automation (RPA): A Primer for Internal Audit Professionals," *https://www.pwc.com/us/en/services/risk-assurance/library/robotic-process-automation-internal-audit.html*
2 KPMG, "Internal Audit and Robotic Process Automation: Considerations for Assessing and Leveraging Intelligent Automation," *https://assets.kpmg/content/dam/kpmg/nl/pdf/2018/advisory/internal-audit-and-robotic-process-automation.pdf*
3 *Ibid*.
4 Struthers-Kennedy, A.; "RPA: First Steps to Greater Internal Audit Efficiency," Corporate Compliance Insights, 16 November 2018, *https://www.corporatecomplianceinsights.com/rpa-first-steps-to-greater-internal-audit-efficiency/*
5 *Ibid*.