Advances in data science, processing capabilities and technology have sparked the fourth industrial revolution. Organizations are rapidly digitalizing parts of their businesses using robotic process automation (RPA) to achieve efficiency and increase quality.

What Is RPA?

RPA is rules-based software programmed to automate activities by performing rules-based tasks. Its best use is with repetitive tasks that interact with multiple applications, occur with significant frequency at significant effort and leverage structured data and formats. RPA operates in the user interface layer and is able to automate rules-based work without compromising the underlying IT infrastructure. RPA replicates human interactions with proven technology, and it mimics common tasks such as queries, cut/paste, merging and button clicks. RPA can be implemented on desktops or in virtual environments and provides flexibility to quickly deploy robots directly onto existing desktops (personal computers, laptops) or virtually (virtual machines) to save on additional hardware costs.

Internal Audit and RPA

Large and small Internal audit (IA) departments have already begun their journeys into the world of automation by expanding their use of traditional analytics to include predictive models, RPA and cognitive intelligence (CI). With automation technologies advancing quickly and early adopters demonstrating their effectiveness, now is the time to understand and prioritize opportunities for automation and take important steps to prepare for thoughtful, progressive deployment.

Methodology to Implement RPA in Internal Audit

RPA assessment typically involves inventorying, prioritizing and vetting processes for suitability. All processes technically or economically infeasible should be filtered out as soon as possible by gathering baseline information and pragmatically identifying inhibitors to automation. The criteria with the matrix of process automation and value creation should be defined for qualitative and quantitative assessment to shortlist the qualified processes.

Fully qualified processes should be used to create a business case with complexity and implementation cost to justify pursuing RPA implementation. RPA implementation typically follows the Agile methodology with the following stages:

1. Define and design
2. Build and refine
3. Test and deploy

Hassan Toor, CISA, ACA, CFE, FCCA, PMP

Is an independent consultant. He has been associated with Deloitte and PricewaterhouseCoopers (PwC). Toor has extensive experience working within the enterprise resource planning (ERP) risk domain. In addition, he has experience with information risk management, software license management, project risk and quality assurance for major ERP products. Toor also has extensive knowledge of core internal audits, process and system optimization.
A project's scope, requirements, budget, timeline and approach should be clearly defined at the define and design stage. During the build and refine stage, the implementation team iteratively develops the complete product in potentially deployable increments and increases efficiency through frequent feedback and improvement cycles. Features are continuously designed, developed, tested and integrated leading to increasingly complete and stable builds. The team may increase the efficiency by identifying effective practices and adjusting to resolve what went wrong during this phase. During the last stage, test and deploy, the product or solution is mature enough to be deployed to the end-user domain. This typically requires that a usable subset of the product or solution has been completed to an acceptable level of quality and that user documentation is available supporting the transition.

The importance of documenting the project and all deliverables is critical for any RPA project. If an organization wants to involve a third party for RPA assurance, these deliverables will be critical for understanding and getting assurance that RPA is working as per the intended objectives.

RPA Utilization During the Risk Assessment Stage of Internal Audit

Organizations conduct risk assessments to identify different types of organizational risk. For example, they may conduct risk assessments to identify strategic, operational, financial and compliance risk to which the organization is exposed.

RPA can be used to transfer the results from the spreadsheet of risk assessment of auditable processes, functions and units within the organization to the planning worksheet. This could save important hours of work for auditors and the risk assessment plan will remain updated at any given time of the year.

RPA Utilization During the Fieldwork Stage of Internal Audit

During this phase, the audit team performs the audit. Some of the procedures generally performed during fieldwork are as follows:

- Review supporting documentation.
- Perform analyses.
- Identify exceptions.

The following examples have been extracted from the fieldwork stage of different audits to be mapped with RPA and automate the IA department:

- RPA can be configured to identify and respond to potential fraud such as money laundering using automated rules-based monitoring of transactions (e.g., flagging activities for auditors' review), which helps auditors focus on other risk areas.

- RPA can help detect suspicious logs associated with IT systems. Gathering audit documentation/evidence is a semi-manual process that is time consuming and very detail-oriented. Automatically gathering documentation of business processes and IT systems, transactions and controls helps provide continuous assurance, thereby enabling quicker corrective action.

- One particular set of US Sarbanes-Oxley Act (SOX) controls testing relates to user access of systems. The prescribed test plan has historically been largely manual and must be executed quarterly. Automation through RPA augments existing manual effort by relieving strain on human resources.

- On an annual basis, management teams perform time intensive manual testing over system configurations (i.e., security settings). RPA configuration minimizes effort to populate work papers, which historically is a non-value added activity, and enables auditors to focus solely on issue confirmation and evaluation.

- A significant amount of manual effort and time can be spent reviewing each expense report and supporting receipts for validity and accuracy. RPA can be used to drastically reduce hours per year of manual review and improve audit compliance.

- RPA can help to audit entire populations rather than the samples. Tests can be run consistently and automatically to get results that can be analyzed for an exception or anomaly in the test.

- RPA can be configured to perform the reconciliation of data from a different system, which could save hundreds of hours during each audit.
The above examples are starting points to initiate the RPA discussion. The final selection of processes and steps should be based on an organization's preference and alignment with the objective of the IA department.

**RPA Utilization During Audit Closing and Follow Up**

A summary of audit findings, conclusions and specific recommendations are officially communicated during audit closing. The following two aspects can be automated with the help of RPA:

1. Audit teams spend significant time sending, tracking and receiving responses to confirmations from stakeholders. This is a highly manual process that could result in mistakes and delays.

2. Gathering of audit documentation/evidence is a tedious, time-consuming process and very detail-oriented. Audit document archiving can be best automated with the help of RPA during the closing of an audit.

IA follows up on all audit findings within one year of when the report was issued. RPA can save thousands of hours per year for follow-up audits. It will improve audit quality and reduce human error by managing documents automatically.

**Key Considerations During RPA Implementation**

RPA implementation is an important step toward process digitization, but it creates additional risk for the organization. Some important considerations for the IA department are:

- During RPA implementation, securing accounts provisioned for bots, segregating duties, password management governance and access attestations are critical.
- Automation continuity planning becomes needed as human dependency on automated work steps increases.
- Testing strategies need to consider data quality, upstream/downstream dependencies on systems and human actions.
- The ability for non-technicians to develop automations creates a need for governance of development activities, release management and coding standards.
- The governance structure needs to consider both the scaling approach and the risk control management of automation.
- Generic bot identification often poses risk of noncompliance to software licenses due to potential indirect usage.

**Conclusion**

As organizations adopt new technologies and embrace new business models, they also need to evolve their culture, working practices and organizational structures. Transforming the organization, and the risk/control management functions, in a way that is deliberate and controlled is critical to achieving strategic objectives. RPA can assist IA to generate and standardize data to run custom analytics, automate the initial data gathering and classification for the annual risk assessment process, test of details that consist of data fields matching from one source to the other, and automate controls testing thorough bots. In addition, RPA assists in tracking outstanding evidence, follow-up requests and management responses.

The IA department can save important man hours by employing robots to perform a number of repetitive tasks discussed here. This can help IA focus on unique, important tasks to achieve a deeper, more sophisticated analysis of risk as part of the audit process.

**Endnotes**