



RPA AND THE GOVERNMENT AUDIT

By Isa I. Farhat, CPA

As government programs evolve, and agency missions grow increasingly complex, governments are increasingly reliant upon technology to support strategic, operations, compliance and reporting objectives. Faced with unprecedented disruption of the “old ways” of achieving these objectives, agencies have increased use of robotic process automation (RPA) — computer-coded, rules-based machines to automate repetitive, rules-based human tasks. In the simplest terms, RPA uses robots, or “bots,” to record human actions, then follow prescribed protocols and procedures with precision for increased compliance and cost efficiencies.

However, as agencies embrace RPA, specific audit implications need to be considered by government and addressed by auditors to enable successful transformation. Since the audit may directly affect critical funding required to execute complex missions to serve constituencies, agency leadership must gain an understanding of the many aspects of RPA that can elevate risk exposure, such as changes inherent post-automation, job role changes and related

internal controls, access security and application change management, and governance of the RPA-enabled environment. Therefore, RPA must be meticulously scrutinized by auditors, as current auditing standards related to RPA are not yet established.

How Is Government Using RPA?

In its January 2018 blog post, “We’re Thinking about Robots,”¹ the U.S. Department of the Treasury’s Bureau of Fiscal Service (Fiscal Service) noted that the Office of Financial Innovation and Transformation (FIT) was tasked with piloting a project² to explore ways RPA could improve financial processes in the bureau. The pilot³ discovered an average 60 percent improvement in the amount of time it took to finish all tasks in the seven processes that were automated. In addition, throughput increased by 30 times, and processing capacity was created without adding human resources. Because RPA performs tasks exactly as defined (assuming bots are properly configured), accuracy in carrying out automated tasks reached 100 percent.

Figure 1. Fundamental Principles Underlying the Auditors' Risk Assessment

- 1 Professional skepticism and brainstorming;
- 2 Involvement of appropriate engagement team members;
- 3 Understanding of the entity and its environment, including internal control components and the impact of information systems on inherent risk;
- 4 Identification of relevant risks of material misstatement, including fraud risks;
- 5 Designing further audit procedures to respond to the identified risks of material misstatement;
- 6 Risk assessment as an iterative process across the five Green Book components;
- 7 Appropriate audit documentation that connects the auditors' risk assessment, professional judgment, and design and execution of audit procedures.



Accounting is the most common area of RPA deployment in government, and this functional area of government is well-suited for many types of automation. For example, traditional RPA that automates transactional processes in accounting or enhanced finance and controls automation, often referred to as “last mile of finance” automation, work well for a variety of reasons, including:

- Need for a high degree of accuracy and consistency;
- Repetitive, manual nature of transaction processing;
- Information gathered from fragmented systems;
- Dependency on data entry, data manipulation and report generation.

The Changing Regulatory Landscape

With increasing use of emerging technologies such as RPA, many regulatory bodies and standards setters have begun to assess them and form “regulator’s perspectives.” In prepared remarks⁴ given at the 43rd World Continuous Auditing and Reporting Symposium on November 2, 2018, Kathleen M. Hamm, a member of the Public Company Accounting Oversight Board (PCAOB), said innovative uses of technology offer the potential to

fundamentally change not only the financial reporting process, but also the audit. She also said technology offers the promise of improving audit quality plus the opportunity to proactively develop accounting and auditing standards and regulatory requirements into solutions. Already, the newly revised Office of Management and Budget (OMB) Circular No. A-123, *Appendix A – Management of Reporting and Data Integrity Risk*,⁵ emphasizes data as an asset and requires more rigor related to compliance with the Digital Accountability and Transparency Act (DATA Act).

Moreover, at the American Institute of Certified Public Accountants (AICPA) conference on current developments at the Securities and Exchange Commission (SEC) and PCAOB, SEC officials stressed the importance of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework⁶ Principle 9 to maintain effective internal controls over financial reporting, particularly in a period of change like RPA implementation. Therefore, government financial managers should prepare for auditors to focus on the following areas in their financial statement audits:

- Understanding the changes resulting from processes that have been automated and reevaluating risks through risk assessment;

- Technology reliability within business processes, including automated controls;
- Information system controls, including those for access and bot credentialing, change related to maintaining bots, business continuity planning, and other general controls;
- Accuracy, security and completeness of stored data, including data leakage and privacy;
- Cybersecurity and procedures for cyber-incident response;
- Segregation of duties between bot IDs and end users;
- RPA governance, including monitoring of bot throughput, processing errors and exception handling through human intervention (i.e., partial automation);
- Completeness and accuracy of transactions processed through RPA, considering configuration, parameters of reports, and processing logic.

The Auditors' Risk Assessment⁷

Auditors must seek to understand automated transactions in the entity’s operations that are significant to financial statements as well as

related control activities. This can be conducted in walk-throughs of the automated processes and by understanding the related parameters, logic and source data that the automation encompasses.

It is important for auditors to understand those transactions that give rise or contribute to risks of material misstatement in financial statements (see **Figure 1**).⁸ This includes a consideration of whether automation of transaction processing would result in modification of the nature, timing and extent of auditors' procedures. The information obtained from risk assessment would form the basis for the design of further audit procedures to respond directly to each risk.

Adaptation to Addressing RPA in an Audit

Despite the evolution of RPA in accounting and finance, regulators remind auditors that the fundamental financial reporting framework does

not change. If a significant amount of an entity's financial information is electronically initiated, recorded, processed or reported, substantive audit procedures alone might not provide sufficient evidence for auditors for a relevant financial statement assertion. In other words, when RPA is used to meet financial reporting or internal controls requirements, auditors must comprehend the design of that technology. Effective internal controls are essential to mitigate potential for improper initiation or alteration of information. These actions can go undetected when recorded, processed or reported in electronic form alone.

Regulators have cited challenges, such as technology that does not operate as intended due to coding errors when developed or intentional or unintentional changes made after the technology is deployed. In addition, in changing environments, computer code underlying complex technology can degrade over time, becoming less responsive. As a result, processes

should be in place to continuously monitor and confirm that the output of an application remains consistent with expectations.⁹

Accordingly, audit firms have begun asking their clients specific questions during the planning phase of an audit, such as: "Have you implemented or do you plan to implement any emerging technologies to support financial reporting (for example, cloud computing, RPA or blockchain)?" This helps auditors gain a better understanding of RPA tools in the IT environment, which can impact evaluation of the design of internal controls.

Consideration of Risks and Internal Controls

Government agency leaders should consider the revised OMB Circular A-123, particularly its requirements for enterprise risk management (ERM), which requires increased focus on developing and utilizing a risk-based approach to achieve agencies'



OUR EXPERIENCED TEAM IS DEDICATED TO YOUR CONTINUED SUCCESS

TURN TO AOC'S TEAM OF EXPERTS TO TACKLE YOUR AGENCIES' COMPLEX ISSUES.

ENTERPRISE RISK MANAGEMENT AND STRATEGIC MANAGEMENT

AUDIT READINESS FOR DEFENSE AND THE INTELLIGENCE COMMUNITY

INTERNAL CONTROLS, MONITORING AND DATA ANALYTICS

PROPERTY PLANT & EQUIPMENT VALUATION AND ACCOUNTABILITY

FINANCIAL REPORTING

INFORMATION SYSTEM CONTROLS AND COMPLIANCE

FINANCIAL POLICIES AND PROCEDURES

BUDGET FORMULATION AND EXECUTION

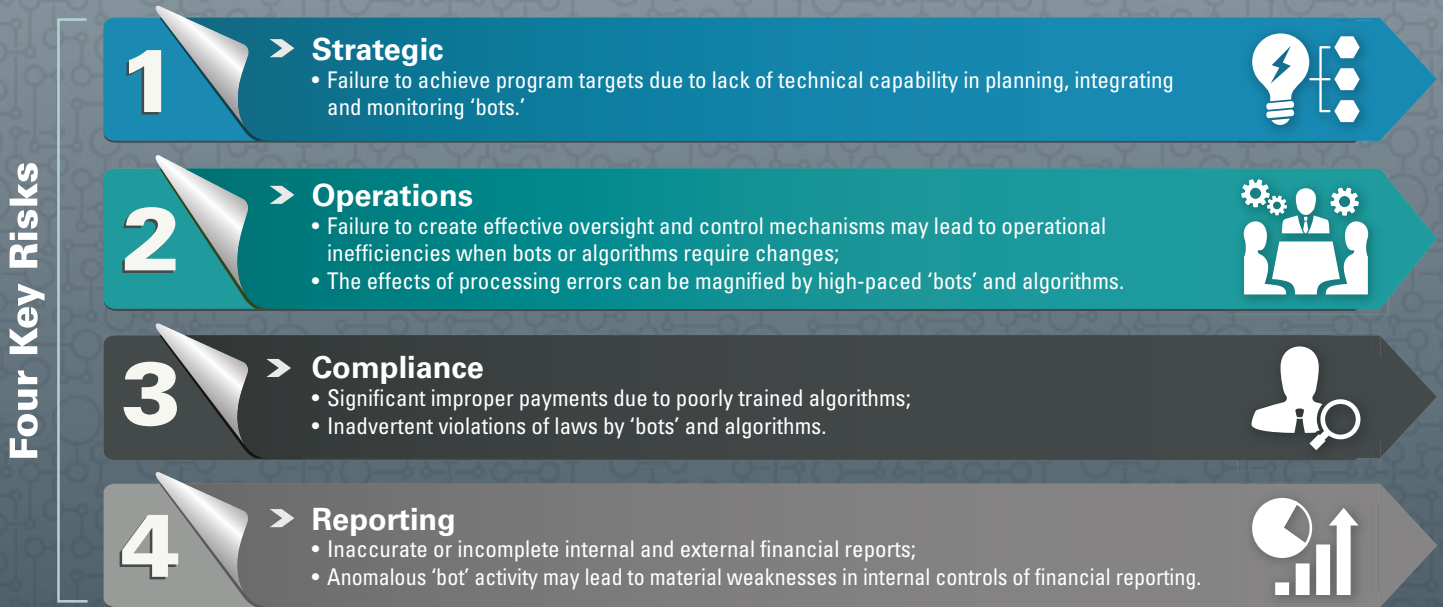
ACCOUNTING OPERATIONS

INFO@AOCSOLUTIONS.COM

AOC SOLUTIONS

WWW.AOCSOLUTIONS.COM

Figure 2. Illustrative Example of a Risk Profile, Adapted from GAO Green Book



strategic, operations, compliance and reporting objectives. RPA solutions may introduce new risks to an organization if not managed appropriately (see Figure 2).

An increased focus on the effectiveness of an agency's internal controls systems related to RPA informs how these systems help achieve objectives. The Government Accountability Office (GAO) Green Book¹⁰ sets standards for effective internal controls in federal agencies. Leaders should follow these standards when assessing RPA, building a business case for it, determining an optimal operating model, identifying RPA solutions, and planning implementation. They should also understand RPA through the lens of internal controls. In audit planning, auditors will seek to understand automated processes as well as internal controls relevant to the audit.

Improper implementation or automation of the wrong processes (e.g., operational risks) may result in immediate financial losses to an agency. Bot-related errors affecting the integrity of cybersecurity programs or compliance with data privacy regulations may not only result in direct costs to the agency, but also cause reputational concerns. Therefore, it is critical to determine how changes inform risk assessment, particularly those risks

arising from IT, and whether modifications to existing standards, processes and structures (e.g., the control environment) are necessary. As agencies implement RPA, it is imperative they perform their own risk assessments associated with the processes being automated, design internal controls for it, and produce appropriate audit evidence.

RPA Governance in Government Agencies

An effective governance model establishes accountability throughout the automation lifecycle, from creation of the automation program to design and testing of bot functionality and outputs to bot implementation and, finally, to monitoring effectiveness of the automation program. It is important to identify an executive sponsor with appropriate knowledge of emerging technologies plus the authority to champion and lead the project in the agency. Oversight bodies may outline and develop a governance structure to encompass the following:

- Establish RPA policies and standards through a governance framework;
- Leverage existing internal controls and enhance and adapt them to the automated environment;

- Define and create access management policies and internal controls for bots to oversee the work of other bots;
- Adapt bots to detect and report errors so that human intervention can occur when needed;
- Manage bots through environment changes by implementing appropriate controls;
- Create compliance policies and tools to monitor and log bot output for enhanced transparency;
- Establish cross-functional working groups and assign responsibility to individuals for maintaining bots and resolving issues.

Achieve Effectiveness and Efficiency

RPA can be an effective solution for automating repetitive tasks, improving processes subject to audit, and contributing to effective risk management. RPA can help an organization achieve effectiveness and efficiencies in executing tasks that are critical to mission support, including timely reporting of financial and operational information and enhanced financial reporting. Bots not

only follow prescribed protocols and procedures with precision, but also can be programmed to capture and maintain complete audit logs and automate reporting for a stronger audit process. Benefits for auditors include access to more audit data in a standardized, reliable, consistent format plus automated reporting that enables auditors to focus on analysis and decision-making, rather than manual data collection and consolidation. █

Endnotes

1. "We're Thinking about Robots." Bureau of the Fiscal Service, Feb. 5, 2018. <https://www.fiscal.treasury.gov/fit/blog/we-are-thinking-about-robots.html>
2. "Bureau of the Fiscal Service Launches Two Innovative Pilot Projects." Bureau of the Fiscal Service, Oct. 2, 2017. <https://www.fiscal.treasury.gov/fit/blog/innovative-pilot-projects.html>
3. "Everything You Want to Know About RPA but are Afraid to Ask." Bureau of the Fiscal Service, July 20, 2018. <https://www.fiscal.treasury.gov/fit/blog/everything-you-want-to-know-about-rpa.html>

4. Hamm, Kathleen M. "Mexican Mangos, Diamonds, Cargo Shipping Containers, Oh My! What Auditors Need to Know about Blockchain and Other Emerging Technologies: A Regulator's Perspective." Nov. 2, 2018. http://raw.rutgers.edu/docs/wcars/43wcars/Sides/Mexican%20Mangos%20Diamonds%20Shipping%20Containers%20Oh%20My.11.02.18%20Hamm_.pdf

5. Shaun Donovan, "OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control" (official memorandum, Washington, D.C.: Office of Management and Budget, 2016), <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf>

6. Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) Internal Control – Integrated Framework, Principle 9, "The Organization Identifies and Assesses Changes That Could Significantly Impact the System of Internal Control."

7. Adapted and updated from *Audit for Robotics, Process Robotics, the risk management framework, and implications for the audit*: <https://www2.deloitte.com/us/en/pages/public-sector/articles/federal-audit-for-robotics.html>

8. "U.S. GAO – Financial Audit Manual", Section 260. U.S. Government Accountability Office (U.S. GAO).

9. Prepared remarks given by Kathleen M. Hamm, Public Company Accounting Oversight Board (PCAOB) Member, at the 43rd World Continuous Auditing & Reporting Symposium on Nov. 2, 2018.

10. "U.S. GAO – The Green Book." U.S. Government Accountability Office (U.S. GAO). <https://www.gao.gov/greenbook/overview#t=0>



Isa I. Farhat, CPA, is a partner in Deloitte's financial risk, transactions and restructuring market offering. He has 21 years' experience in providing audit and

financial advisory services to a range of complex, multinational clients, with a focus on aerospace, defense contracting, manufacturing, professional services and technology industries.



Cotton & Company is chosen and trusted because of the values we live by and the value we provide. Our team works with you to find solutions for today and the future.

Looking for professional audit and advisory services you can trust? Cotton & Company has the answers you need.



www.cottoncpa.com
703.836.6701

Reproduced with permission of copyright owner. Further reproduction prohibited without permission.