Deloitte.

Audit for Robotics

Process Robotics, the risk management framework, and implications for the audit

Federal agencies are facing unprecedented budgetary and regulatory disruption as they manage mounting budget constraints while trying to be more agile to increasing mission objectives. The combination of unfunded mandates, a shrinking workforce, and excessive contractor spend is prompting federal agencies to look for innovative solutions such as Digital Labor[1] to address these challenges. No longer are federal executives limited to the option of simply hiring new federal employees, procuring additional contractors, or implementing expensive technology. Deloitte Process Robotics (DPR) offers an inexpensive Digital Labor solution that can be implemented in weeks and provides the ability to rapidly scale. Simply put, Digital Labor should be thought of as a new category of resources that leaders can tap into—a pool of digital labor that provides leaders with access to new capabilities and options to achieve mission goals. However, as federal agencies begin to embrace Digital Labor and its automation capabilities, such as DPR, there are key audit and risk management considerations that need to be considered and addressed by both the auditor and federal agency executives in order to enable successful transformation.

DPR uses Robotic Process Automation (RPA), which is computer-coded, rules-based software 'bots' to automate human activities for repetitive, rules-based

[1] Digital Labor paper: https://www2.deloitte.com/us/en/pages/public-sector/articles/a-roadmap-for-building-digital-labor.html

tasks. In the simplest terms, the technology uses bots to record actions that a human takes to complete a computer-based task, and then replicates those actions at the same security setting as the user. Bots operate in the user interface layer where they are able to automate processes without compromising the underlying information technology (IT) infrastructure. They follow prescribed protocols and procedures with precision, allowing increased compliance and cost efficiencies. To learn more, please refer to Deloitte's 2015 paper titled Process Robotics[2].

As federal entities begin to consider DPR, audit considerations will, more often than not, quickly become a key topic. Within the federal government the audit directly affects the agency's ability to receive the critical funding required to execute its mission to serve the nation and its citizens. It is important that federal agencies understand that automated processes will be meticulously scrutinized by auditors to ensure that all items and transactions that contribute to external financial reporting are correctly documented.

An auditor begins the audit process with a risk assessment. Risk assessment underpins all aspects of the audit. It is grounded in the auditors' understanding of the entity's industry and environment. Entity-specific factors such as the nature of the entity, its activities and transactions, and its internal controls are all thoroughly examined. Risk assessment procedures are audit procedures that provide the basis for identifying and assessing risks of material misstatement, whether due to fraud or error, and for designing appropriate further audit procedures.

There are seven tenets of an effective risk assessment, as outlined in Figure 1, that are relevant to and present in all effective audits that allow for proper reporting. The two most important judgements that an auditor makes when auditing an environment that uses automation solutions that produce information that ultimately is reported are: understanding the risk around the entity and its environment (including internal controls) and focusing on identifying relevant risks in material misstatements.

The auditor must seek to understand the automated transactions in the entity's operations that are significant to the financial statements as well as the related control activities. This can be conducted through walk-throughs of the processes that are automated and by understanding the related parameters, logic, and source data that the automation encompasses).

Therefore, it is imperative that, as entities implement DPR solutions, finance executives perform their own risk assessment associated with the transactions being automated, design a system of internal controls related to the processing of the transactions that are being automated, and then produce appropriate audit evidence related to the processing of these transactions.

It is important for the auditor to understand what transactions give rise or contribute to risks of material misstatement of the financial statements. This includes a consideration of whether automation of the processing of higher risk transactions would result in modification of the nature, timing, and extent of the auditors' procedures. The information obtained from the risk assessment process forms the basis for the design of further audit procedures that are directly responsive to each identified risk of material misstatement.

7 Tenets of the risk assessment:

1) Auditors' mindset
2) Involvement of the appropriate engagement team members
3) Deep level of understanding of the entity and its environment, including internal controls
4) Focus on the identification of relevant risks of material misstatement
5) Designing further audit procedures that are responsive to the identified risks of material misstatement
6) Recognition that risk assessment is an iterative process
7) Audit documentation that displays a clear connection between the results of risk assessment, the auditors' professional judgments, and the design and execution of the auditors' audit procedures.

Figure 1: 7 Tenets of Risk Assessment

Considerations for the Auditor

An automated environment

If a significant amount of the entity's information is electronically initiated, recorded, processed, or reported, this is often an indicator that substantive procedures alone might not provide sufficient evidence for

[2] Deloitte Process Robotics paper: https://www2.deloitte.com/us/en/pages/public-sector/articles/process-robotics.html

the risks of material misstatement affecting a relevant assertion (e.g., completeness, accuracy, existence, cut-off, among others). According to the American Institute of Certified Public Accountants (AICPA) Standard AU-C 315.31, "In respect of some risks, the auditor may judge that it is not possible or practicable to obtain sufficient appropriate audit evidence only from substantive procedures. Such risks may relate to the inaccurate or incomplete recording of routine and significant classes of transactions or account balances, the characteristics of which often permit highly automated processing with little or no manual intervention. In such cases, the entity's controls over such risks are relevant to the audit and the auditor shall obtain an understanding of them". Furthermore, the potential for improper initiation or alteration of information to occur and not be detected may be greater if information is initiated, recorded, processed, or reported only in electronic form and appropriate controls are not operating effectively.

Considerations for getting started

Look before you leap

Specifically, agency executives must consider Enterprise Risk Management and Internal Control (codified in Office of Management and Budget Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, and the Government Accountability Office (GAO) Greenbook) when assessing for automation opportunities, building the business case for automation, determining an optimal operating model, identifying an RPA solution, and planning the implementation. According to the GAO Greenbook, internal control is a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved. Therefore, federal agency executives should understand DPR through the lens of internal control over financial reporting, and the auditor will evaluate the DPR solution in consideration of the five components of internal control:

- **Control environment**—The foundation for an internal control system. It provides the discipline and structure to help an entity achieve its objectives. DPR is sure to become part of the control environment.
- **Risk assessment**—Assesses the risks facing the entity (including consideration of DPR solutions) as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses, including the consideration of fraud.
- **Control activities**—The actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information system. The design of an effective internal control system, considering controls over the DPR solution.
- **Information and communication**—The quality information management and personnel communicate and use to support the internal control system. Consider the information that DPR provides and how that information is used and communicated in the entity.
- **Monitoring**—Activities management establishes and operates to assess the quality of performance over time and promptly resolve the findings of audits and other reviews. DPR solutions should be subject to management's monitoring.

Conclusion

DPR can be an effective solution not only for automating repetitive processes, but also for improving an entity's processes subject to audit and contribute to effective risk management. Bots not only follow prescribed protocols and procedures with precision, but they also capture and maintain complete audit trails and automate reporting to strengthen the audit process. Benefits for auditors include access to more audit data in a standardized, reliable, and consistent format; and automated reporting that enables the auditors to focus on analysis and decision making (vs. manual data collection and consolidation). A recent Forbes Insights Survey[3] found that 58% of auditors and businesses believe that technology will have the single biggest impact on the audit over the next three to five years. Approximately 59% of the Forbes survey agree that advanced technology will enable a deeper, more sophisticated analysis of data as part of the audit process.

[3] Forbes Insights Survey: https://www.forbes.com/forbesinsights/kpmg_audit2025/index.html

Marc Mancher
Principal
Deloitte Consulting LLP
1919 N. Lynn Street
Arlington, VA 22209
+1 860 488 5071
jmancher@deloitte.com

David McCue
Partner
Deloitte & Touche LLP
1919 N. Lynn Street
Arlington, VA 22209
+1 703 930 0027
dmccue@deloitte.com

Isa Farhat
Partner
Deloitte & Touche LLP
1919 N. Lynn Street
Arlington, VA 22209
+1 301 802 2093
ifarhat@deloitte.com

Roopa Sanwardeker
Senior Manager
Deloitte Consulting LLP
1919 N. Lynn Street
Arlington, VA 22209
+1 571 429 0947
rsanwardeker@deloitte.com

Chris Huff
Senior Manager
Deloitte Consulting LLP
1919 N. Lynn Street
Arlington, VA 22209
+1 571 212 8490
chuff@deloitte.com

Chris Stewart
Senior Manager
Deloitte & Touche LLP
1919 N. Lynn Street
Arlington, VA 22209
+1 571 814 6826
chrstewart@deloitte.com