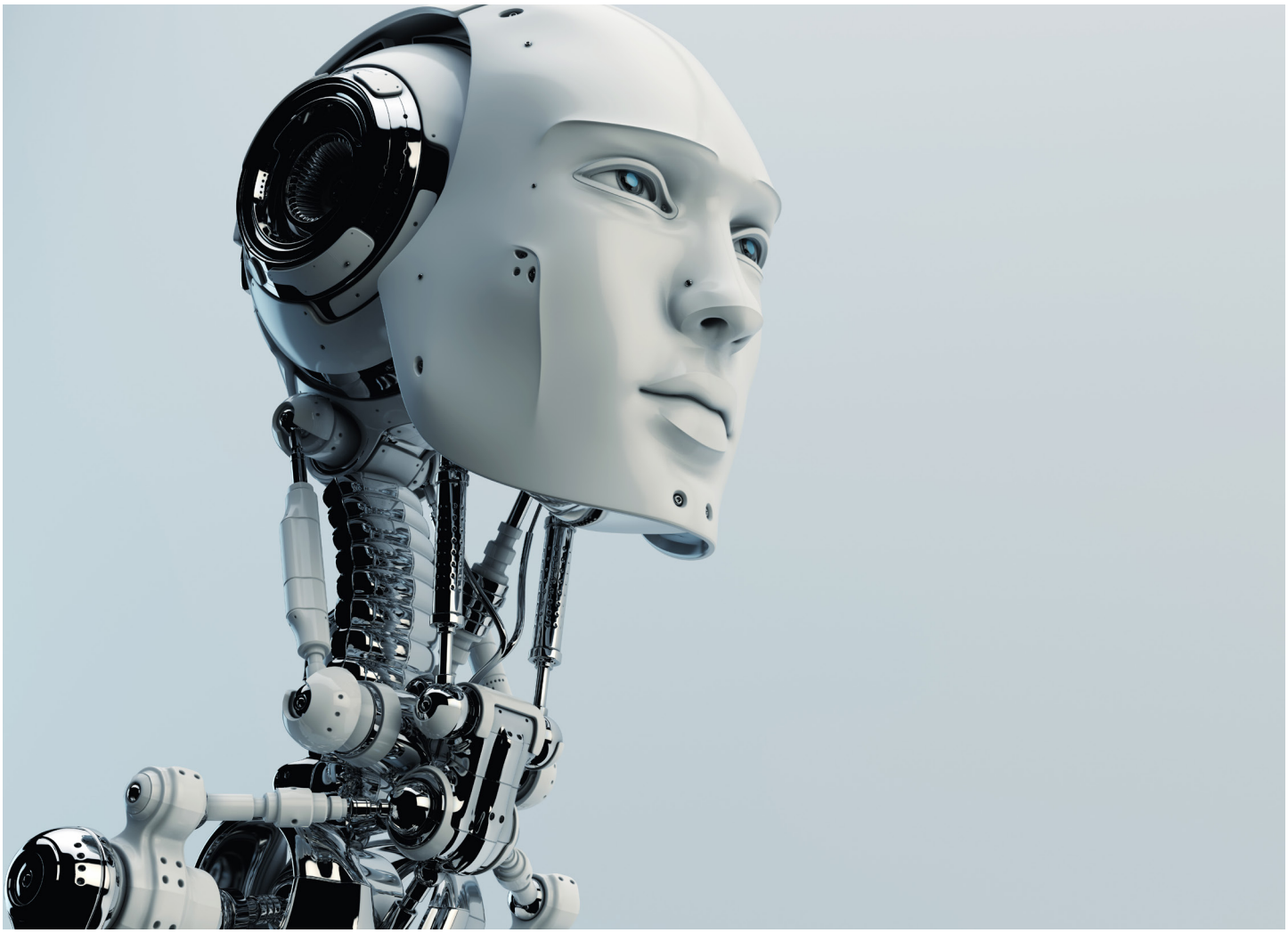
Deloitte.

Refocus your robotic process automation lens

Internal control over financial reporting (ICFR) considerations for developing and implementing bots

How does RPA affect you?



Companies are rapidly digitalizing parts of their business through robotic process automation (RPA). RPA uses computer-coded, rules-based software robots (i.e., bots) to automate certain human tasks. RPA differs from artificial intelligence such as cognitive computing or machine learning because it is unable to learn from data patterns and make judgments. In the simplest terms, a bot is a technology-based solution designed to replicate actions that a human would otherwise take to complete a computer-based task using the same security settings as the user. Bots operate in the user interface layer, where they automate processes without compromising the underlying information technology (IT) infrastructure. Bots follow prescribed protocols and procedures with precision, allowing increased compliance and cost efficiencies (see figure 1).

RPA may be inexpensive to implement compared with other automation technologies and can quickly provide financial and nonfinancial benefits that affect the most common performance measures (see figure 2).

Figure 1. What RPA can do

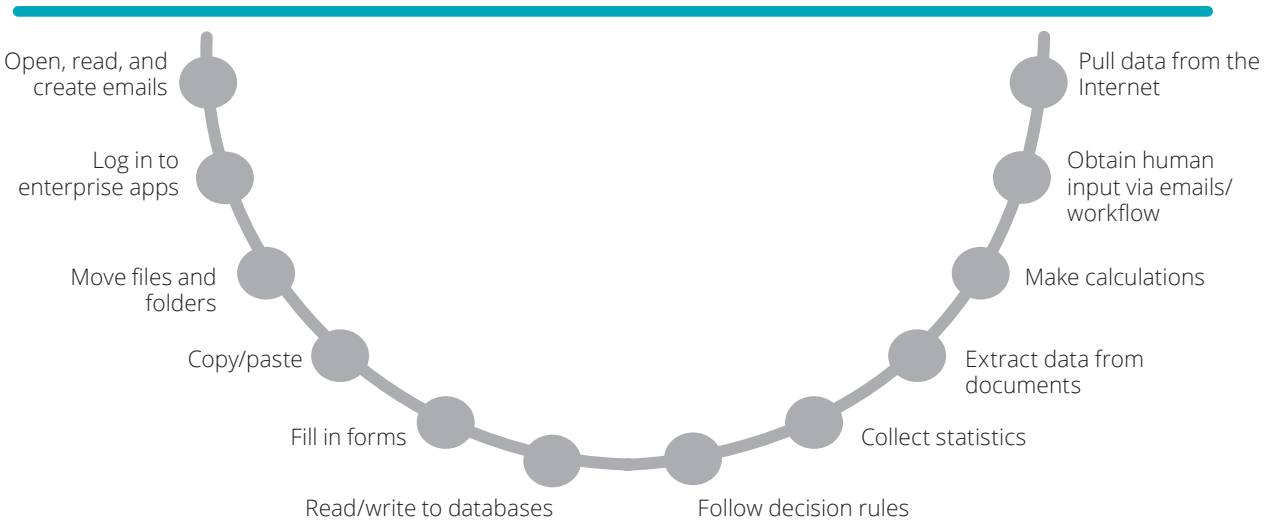
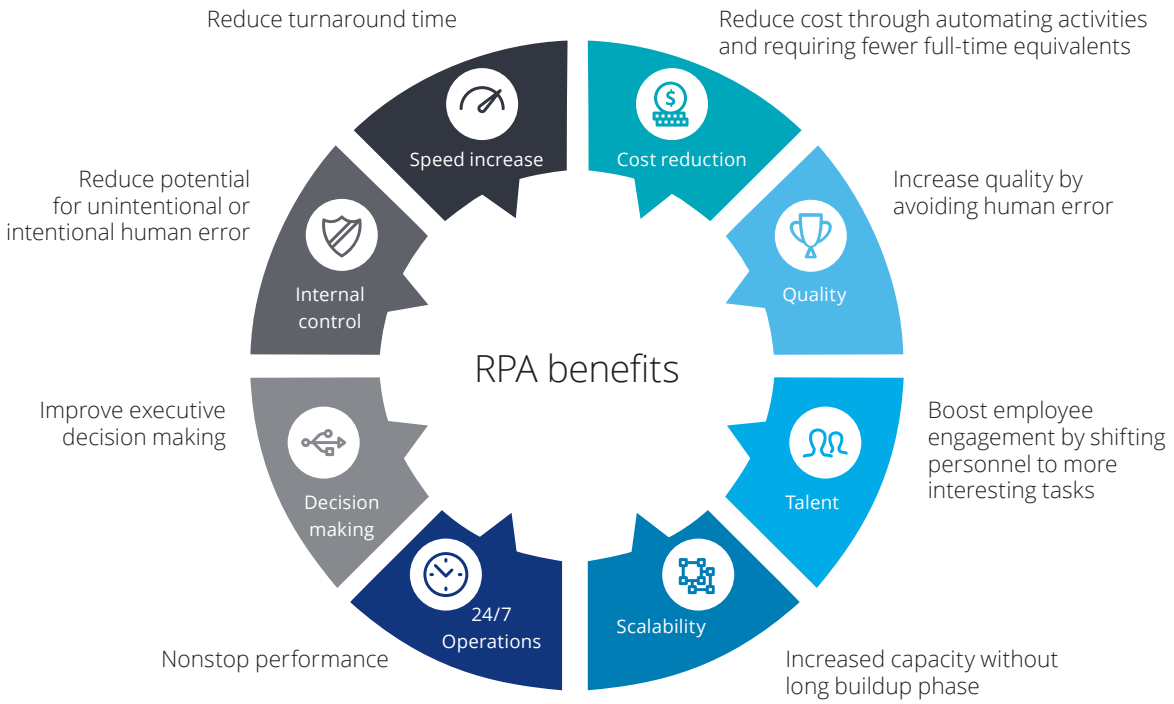


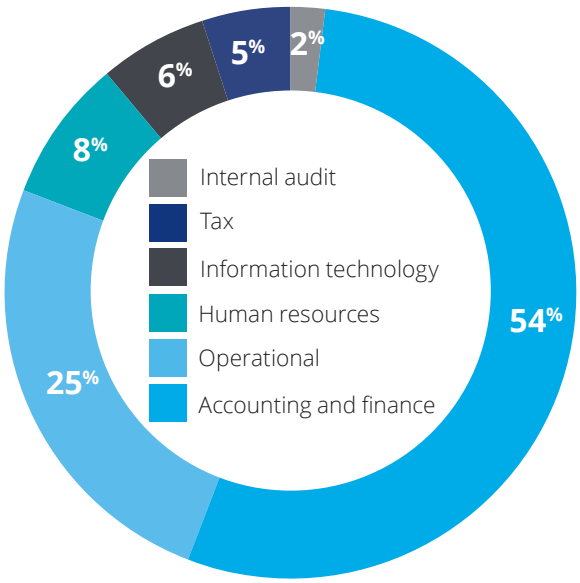
Figure 2. RPA benefits



How are companies using RPA?

According to Deloitte's 2017 RPA survey,[1] market trends are indicating near-universal adoption of RPA in the next five years. Average spending among companies surveyed was $1.5 million for RPA pilots and upwards of $3 million for full-scale programs. This rapid increase in market penetration and spending is contributing to the emergence of a broad ecosystem of RPA vendors and RPA solutions geared toward helping companies capitalize on automation. The use of process automation is at an unprecedented level, as companies continue to identify new ways to use RPA within their organizations. So where are we seeing the most use of automation? The Deloitte Robotics and Cognitive Automation Delivery Center has automated hundreds of unique business processes and identified successful bot deployments in the following areas (see figure 3).

Figure 3. Use of automation



1. David Wright, Dupe Witherick, and Marina Gordeeva, *The robots are ready. Are you?*, Deloitte, 2018, https://www2.deloitte.com/content/dam/Deloitte/bg/Documents/technology-media-telecommunications/Deloitte-us-cons-global-rpa-survey.pdf.

Accounting and finance is the most common area of RPA deployment by our clients. This business function is prime for automation for a variety of reasons, including:

- The 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

Because of these characteristics, a significant number of roles in back-office accounting and finance functions have the potential to be automated. Table 1 below highlights specific processes within the accounting and finance function and the viability of automation within those processes (i.e., low, medium, high).

Table 1. Viability of automation within back-office accounting and finance

Transaction processing				Close, consolidate, and report	
Accounts receivable	**Accounts payable**	**Cash management**	**Project accounting**	**Close the books**	**Legal and external reporting**
Maintain customer master data	Maintain supplier master data	Perform banking & cash mgmt. activities	Perform project accounting	Perform closing	Perform legal and external reporting to regulatory bodies
Manage customer credit exposure	Process invoices	Manage foreign exchange			
Process invoices	Perform payments		**T&E processing**	**Mgmt. reporting**	**Consolidation**
Process payments	Period-end processing and reporting	**General accounting**	Receive & compile reimbursement requests	Perform mgmt. reporting to internal stakeholders	Perform consolidation
Manage collections		Maintain general ledger master data	Audit and document expense reports		
Period-end processing and reporting	**Payroll**	Perform journals	Authorize and process payments		
	Maintain employee master data	Process intercompany transactions			
	Manage payroll		**Tax accounting**		
	Authorize and process payments	**Inventory accounting**	Perform tax accounting		
		Perform inventory accounting			
		Transfer pricing	**Fixed asset accounting**		
		Period-end processing and reporting	Perform fixed asset accounting		
			Period-end processing and reporting		

RPA
- High
- Medium
- Low

Commonly automated accounting and finance functions include:

- Order to cash and accounts receivable
  - Creating and updating customer master data
  - Reviewing and approving customer orders against predefined credit limits
  - Validation and posting of customer payments
- Accounts payable
  - Inputting invoices into an enterprise resource planning (ERP) system
  - Processing changes to purchase orders and updating the ERP system
  - Matching invoices against corresponding purchase orders and receipts
- Financial closing and reporting process
  - Journal entry validation
  - Low-risk account reconciliations
  - Generating reports and loading into reporting/consolidation templates

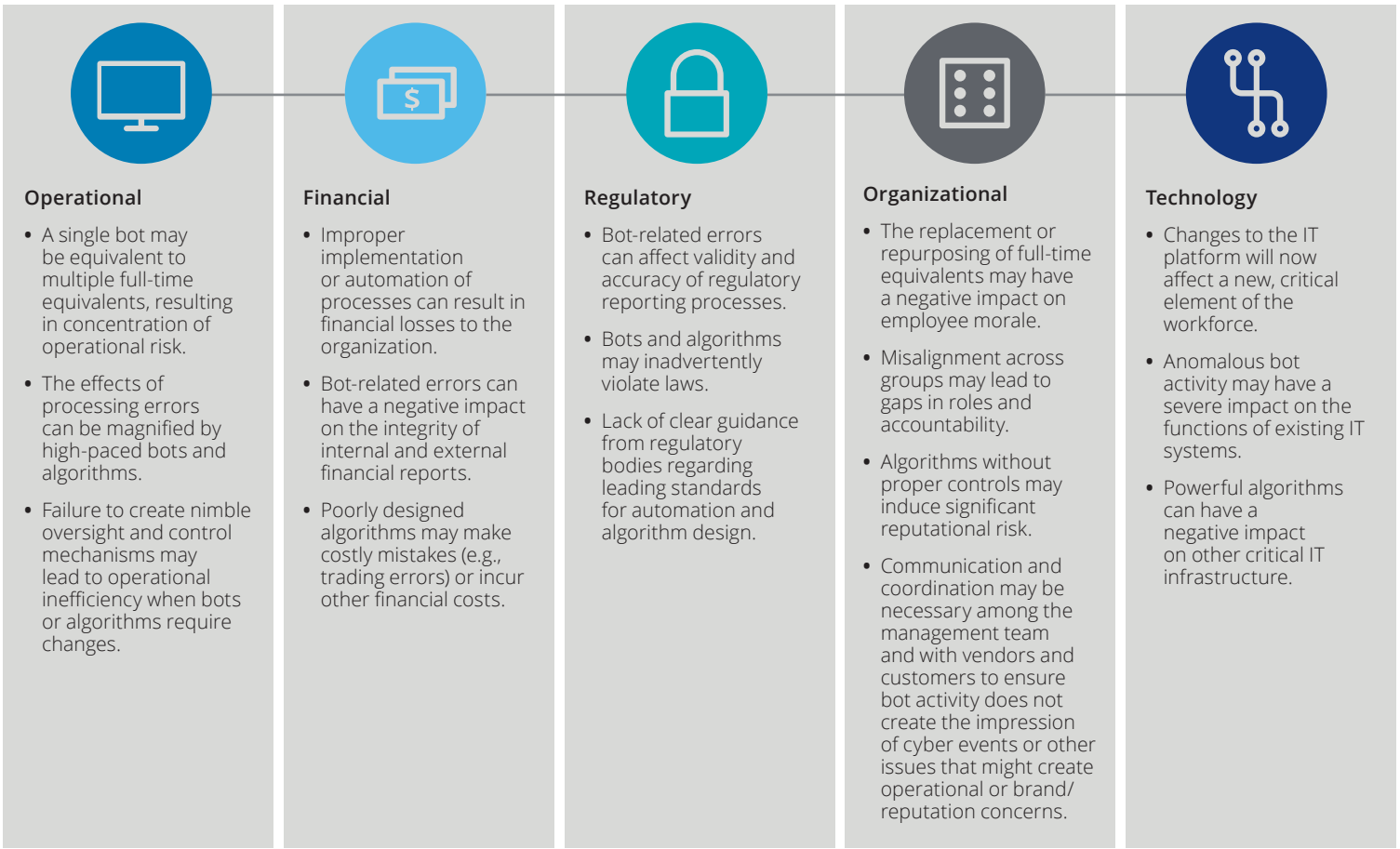
Financial risk and control considerations of RPA

Successful businesses continually work to identify solutions that create operational efficiencies. One trend over the past two decades has been to offshore skilled and nonskilled work as a form of labor arbitrage to reduce costs. Enterprises are now pivoting toward automation of certain business tasks (e.g., account reconciliations, invoice processing, recalculations, source data matching, threshold application) to further disrupt the human capital leverage model. Specifically, RPA may replace or enhance certain tasks previously performed by humans with bots that are cheaper, more efficient, and more reliable.

Although RPA may reduce unintentional or intentional human errors, the implementation of bots presents new risks that businesses need to understand and address. A key risk presented by the rapid adoption of bots is an organization's failure to consider the effects of these operational changes on its internal control over financial reporting (ICFR), specifically those controls over IT. Failure to adequately assess/identify and manage these new risks may erode or limit the value created by this automation arbitrage. Bot-related risks may increase when external third-party systems, websites, and collaboration tools are involved.

To realize the full benefits of automation, businesses should consider how RPA affects risks in a number of categories (see figure 4).

Figure 4. RPA areas of key risks



Source: 2017 MIT SMR and Deloitte Digital business research

Issues arising within any of these risks may lead to financial loss. For example, improper implementation or automation of the wrong processes (i.e., operational risks) may result in immediate financial losses to an organization. Bot-related errors affecting the integrity of cybersecurity programs or compliance with data privacy regulations may not only result in direct costs to the business, but also give rise to reputational concerns in the marketplace. Therefore, it is critical for organizations to assess how these changes inform their risk assessment, particularly those risks arising from IT, and whether modifications to their existing standards, processes, and structures (i.e., control environment) are necessary. When exploring the adoption of RPA technologies, it is important to leverage the existing control environment, when possible, and challenge those areas in which the governance construct may not adequately support these changes. Companies may consider controls in the following layers, in terms of the life cycle from ideation and creation of a bot to implementation and monitoring (see figure 5).

Figure 5. Entity-level controls

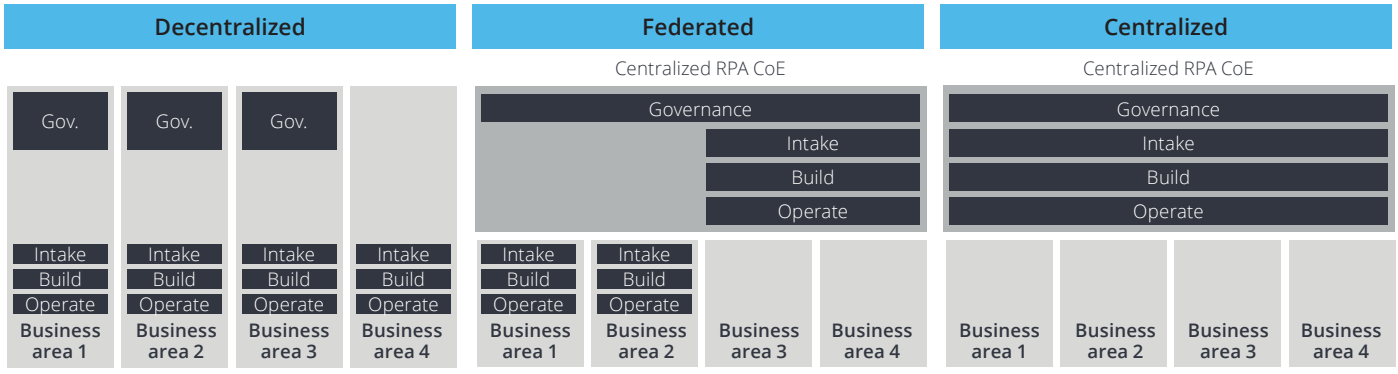
RPA may significantly change the way in which organizations execute day-to-day operations, certain areas of internal control, or both. At the 2017 AICPA Conference on Current SEC and PCAOB Developments, professionals in the SEC's Office of the Chief Accountant emphasized the importance of considering Principle 9 of the COSO framework as part of maintaining effective ICFR, particularly in a period of change, such as the implementation of robotics and other new technologies. Focusing on Principle 9 will help companies prepare for implementation, including establishing an appropriate governance framework that will ensure a smooth transition to managing RPA throughout the business.

An effective governance model establishes accountability throughout the RPA life cycle, from ideation of the RPA strategy, to design and testing of bot functionality and outputs, to implementation of the bot(s), and to monitoring of bot effectiveness. It is important to identify an executive sponsor with the appropriate competency and authority to champion and lead the project. Those charged with governance may outline and develop a corporate RPA charter that includes:

- Type of operating model (decentralized, centralized, federated)
- Standards and policies related to the selection, development, and use of bots within the organization, including success measurement criteria and key performance indicators
- Education and training programs to help management; business owners, including those overseeing bot implementation ("bot managers"); and the internal audit function develop a sufficient understanding of how bots affect risk assessment and the determination of which new or modified controls are necessary for automation and monitoring

The "right size" operating model may consider factors, including RPA capability maturity, availability of resources, the design of the underlying IT infrastructure, and the commonality of RPA needs across the organization. Companies with extensive RPA experience may deploy a decentralized governance model allowing for more autonomy within each business segment, whereas a centralized, federated, or hybrid of the two may be recommended for organizations that are working to mature their RPA capabilities. Table 2 illustrates how these factors may influence the selection of an operating model (decentralized, federated, and centralized).

Table 2. Decentralized, federated, and centralized models



- RPA is a mature capability across many business areas.
- Many business areas have resources with the requisite RPA skill set.
- RPA capabilities and tool needs are business-specific with limited overlap.
- Business area platforms and technologies are siloed.

- RPA is a mature capability in one or more business areas.
- Some business areas have resources with the requisite RPA skill set.
- Some business areas have RPA tool needs that are not applicable to others.
- Business area platforms and technologies are siloed.

- RPA capabilities are not mature across business areas.
- Availability of resources with requisite RPA skill sets is limited.
- Proliferation of RPA capabilities and tools across business areas is limited.
- Platforms and systems across business areas are common.

Development phase

Following the established process selection standards and development methods (from test to production) is essential for the automation tool to achieve the desired outcome. After a bot is placed into the production environment (i.e., the end-user stage in which robotics are put into operation), control activities are needed to mitigate the risks that the software bot is designed ineffectively or the designed automation does not continue to operate to achieve the identified objective. In these situations, it is helpful to analogize the use of RPA technologies in the financial reporting process to designing and implementing automated controls that support a business cycle. Testing the design of the automated control involves a baselining process over the coding and configuration settings behind the automation (as applicable). This process helps confirm that the design follows the business logic defined by the company, including the policies over the identification and reporting of exceptions. Bots should be configured to detect and report errors and raise exceptions to bot managers, addressing these issues in real time. Once RPA development is final and baselining efforts are completed, general information technology controls (GITCs) will ensure that the bots continue to operate as designed.

Implementation phase

Upon implementation, companies will need to contemplate the effects of RPA on their IT risk assessment. The use of RPA presents new risks related to proper security of the access rights assigned to the bots and oversight of any changes to the technology to ensure it continues to operate as designed. Thus, it is critical to obtain a comprehensive understanding of the elements of the IT infrastructure (e.g., database, operating system, network) designed to support the automation technology and the GITCs over those elements, including controls over:

1. Access security — Understanding user roles and system and data access needs for bots interacting with core systems will prevent unauthorized users from accessing RPA's data processing rule sets and the connected data sources. It is important to prevent such unauthorized access because it can be used to access confidential data and manipulate the bots and their automated tasks. Role-based access controls enable organizations to restrict access and authenticate users, thereby segregating automation-related duties among employees. The ability to develop or manipulate the actions of bots can be assigned on the basis of an employee's position within the company. User access controls generally consist of (a) periodic reviews of user access rights and (b) authentication controls over user identification.

2. System change — We generally recommend that preparers follow their existing change management program for software development life cycle–related activities. Change management procedures need to account for bots that use the application undergoing a change. A robust change management program also includes a process for executing changes directly to the bots.

3. Data center and network operations — Providing for the integrity of the information that is processed, stored, or communicated by the relevant aspects of the IT infrastructure is critical to maintaining effective ICFR related to bots. In addition, companies may need to evaluate third-party data privacy concerns when a bot stores data in the cloud.

Monitoring phase

Designing mechanisms to monitor bot effectiveness is critical to controlling and sustaining these changes to the business. Effective oversight and monitoring programs are also paramount to management's ability to assess the effectiveness of bots supporting ICFR and will thus enhance the ability to comply with Section 404(a) of the Sarbanes-Oxley Act of 2002. Therefore, companies may look to a multilayered monitoring approach, including the following control activities:

- Designing audit and compliance protocols to include automation components.
- Continuing the manual business control to validate successful completion of the automated task.
- Reviewing the RPA platform(s) audit logs to verify the validity and appropriateness of each action performed by the bots. This also enables businesses to retrace and remediate issues that result from bot errors or malicious code.
- Performing an annual review of the automation algorithm(s) (i.e., reestablishing the baseline) to confirm alignment to the defined business objective.
- Soliciting periodic feedback from both internal and external audit functions.
- Maintaining a comprehensive compliance checklist to meet regulatory requirements.

Companies may consider reducing the number of monitoring activities over time as their RPA capabilities mature and they sustain long periods of bot effectiveness. For example, companies may decide to remove the manual business control activity and solely rely on automation as management becomes more confident in the overall effectiveness of the RPA program.

Be external audit ready

In addition to management's annual assessment of the company's ICFR, it is important to keep external audit requirements in mind. Success in this area requires proactive communications with auditors throughout the journey to develop and implement RPA.

Holding planning meetings and regular update discussions about the ICFR implications are encouraged practices to help preparers and auditors align their thinking regarding risk assessment and the identification of relevant controls. This will streamline the audit process and build auditors' confidence in the effectiveness of the bots. Some additional topics to consider when preparing for external audits include:

1. Those charged with internal compliance (e.g., internal audit function, IT compliance) should maintain an updated listing of bots and establish a protocol to confirm that updates to processes/controls are reflected in bot design, when necessary.

2. Accounting procedures, process-flow diagrams, and internal control documentation should clearly articulate where and how bots are used within the accounting and finance organization.

3. Strong controls of bot design and operation do not mean a company can neglect controls over inputs and outputs. Proper control frameworks should include controls of the entire transaction cycle, including source data, bot outputs, and points where human intervention is required, such as investigating exceptions or making judgments. This is especially important when bots have a direct impact on financial reporting.

4. Certain bots may be purely operational and only used on the periphery of the financial reporting process, whereas other bots may directly affect accounting and financial statement review control activities. Auditors will need to understand the nature and impact of bots employed by the accounting and finance organization so they can focus their procedures on those most relevant to the financial statements.

Contact us

If you have any questions about the information in this publication, please contact us:

Scott Szalony
Partner | Audit & Assurance
Deloitte & Touche LLP
+1 248 345 7963
sszalony@deloitte.com

Nick Thurber
Manager | Audit & Assurance
Deloitte & Touche LLP
+1 313 394 5533
nthurber@deloitte.com

Kyle Sewell
Senior Manager | Audit & Assurance
Deloitte & Touche LLP
+1 404 201 0759
ksewell@deloitte.com

Patricia Salkin
Managing Director | Risk & Financial Advisory
Deloitte & Touche LLP
+1 609 806 7279
psalkin@deloitte.com

Eriko Sato
Senior Manager | Audit & Assurance
Deloitte & Touche LLP
+1 212 653 6589
erisato@deloitte.com

Michael Corrao
Managing Director | Risk & Financial Advisory
Deloitte & Touche LLP
+1 714 913 1082
mcorrao@deloitte.com

Jeffery Aughton and Stefan Ozer assisted in the production of this publication.

Deloitte.