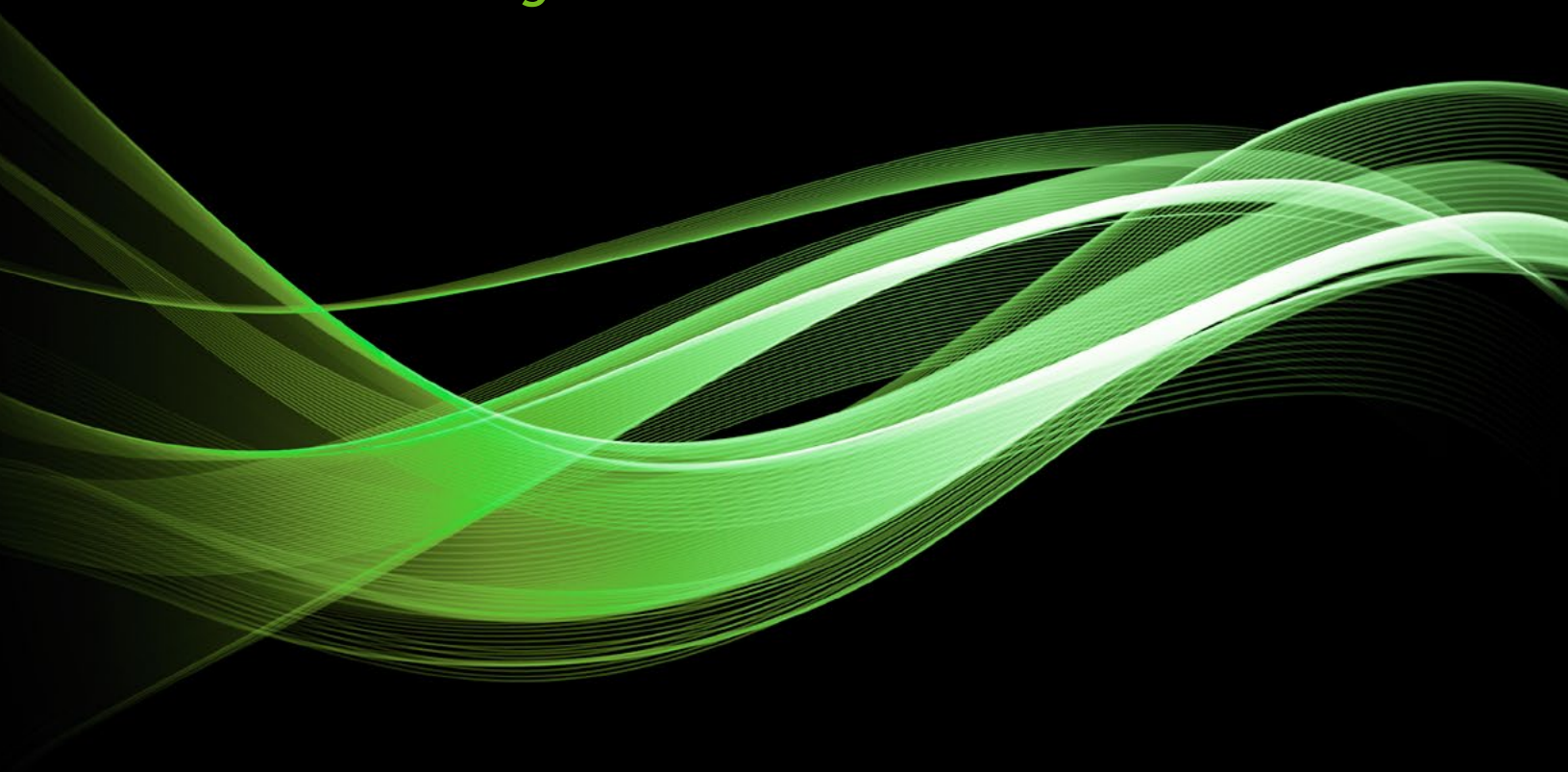
Deloitte.

Moving Internal Audit Deeper Into the Digital Age: Part 3

Beyond Theory — Scaling Automation Capabilities in Internal Auditing



INTERNAL AUDIT FOUNDATION™

Deloitte.

Published by the Internal Audit Foundation
1035 Greenwood Blvd., Suite 149
Lake Mary, Florida 32746, USA

The IIA's International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The IIA and the Foundation work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today's business world. Much of the content presented in their final reports is a result of Foundation-funded research and prepared as a service to the Foundation and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or the Foundation.

ISBN-13: 978-1-63454-118-3
24 23 22 21 20 1 2 3 4 5 6

Contents

Moving Internal Audit Deeper Into the Digital Age: Part 3

Beyond Theory—Scaling Automation Capabilities in Internal Auditing

Automation and cognitive technologies open the door to a level of efficiency and throughput never experienced before. As discussed in the previous two parts of this series, internal audit (IA) has a growing number of modern automation tools at its disposal, which can be used to expand audit scope, provide data-driven insight, and increase risk coverage. However, it's one thing to deploy a digital tool to enhance a specific process or control and entirely another to implement an automation program aimed at transforming the IA organization and moving it deeper into the digital age. The devil is in the details of widescale enablement, which requires humans to change alongside the technology.

Effectively scaling analytics and automation capabilities requires a thorough understanding of what automation is and isn't, along with focus, long-term commitment, and a clear vision of what a digitally enabled IA team looks like. It also requires bottom-up engagement across the entire IA team as well as a new mindset for auditing automation, as detailed in the second installment of this series, *Moving Internal Audit Deeper Into the Digital Age, Part 2: What Internal Audit Needs to Think About When Auditing Automation*. Operational challenges such as access to data, availability of development resources, the complexity of the technology landscape, and changes in audit requirements can also stand in the way.

The following six-step approach has been designed to assist IA leaders in overcoming these common hurdles to implementing a digitally enabled IA operating model. With them, IA leaders can more confidently begin to move analytics and automation beyond theory and toward actualization of the ultimate goal: creating an agile, insightful, and resilient IA organization that adds value to the business.

Strategic Vision

As IA moves deeper into the digital age, the IA organization needs a strategic vision as its "North Star" for digital transformation. What does success look like for your program? Why are IA groups investing so heavily in analytics and automation capabilities? Common strategic goals include expanding risk coverage, decreasing manual testing hours, and gaining and sharing new insights with business clients and stakeholders. Organizations have different opportunities and motivations, and many of them can be achieved with

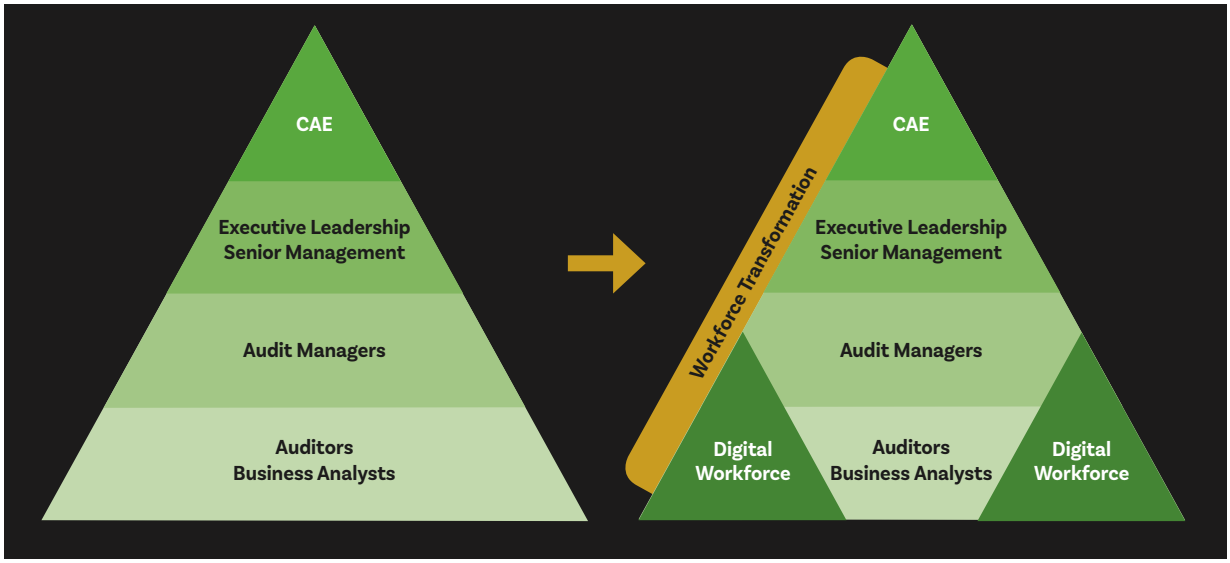
various types of automation and cognitive technologies, not just robotic process automation (RPA).

Achieving this strategic vision requires unwavering commitment and consistent messaging from IA leadership, as well as the appropriate acquisition and alignment of human and financial resources. Often, digital transformation is more about modifying a long-established culture than it is about acquiring new skills or buying new software. Change can be difficult, since inconsistencies and biases can be rooted deep within language, audit methodologies, and incentives.

Not only is it essential to have a sound automation and analytics operating model, it is also important to have a strategy that supports and uplifts the existing workforce. Digital tools such as scheduled scripts, RPA, and artificial intelligence (AI) should not operate in silos, but rather they should work in tandem with the IA organization as a "digital workforce." For example, AI and RPA can be used to execute business-controls automations, perform data quality checks, prefill audit workpapers with system-generated metrics, and assist with Sarbanes-Oxley testing.

When auditors work alongside the digital workforce, IA departments can go beyond traditional table views to analyze data across multiple dimensions without bias while improving audit efficiency and building organizational resilience. Furthermore, the digital workforce can be scaled up or down as the business grows without incurring many of the traditional recruiting and training costs. Over time, the organization can become progressively more efficient. As it matures, it can also move away from sample-based testing and toward full-population testing—removing the guessing game while increasing the accuracy, completeness, and timeliness of audits. See **figure 1**.

Figure 1: Workforce Transformation

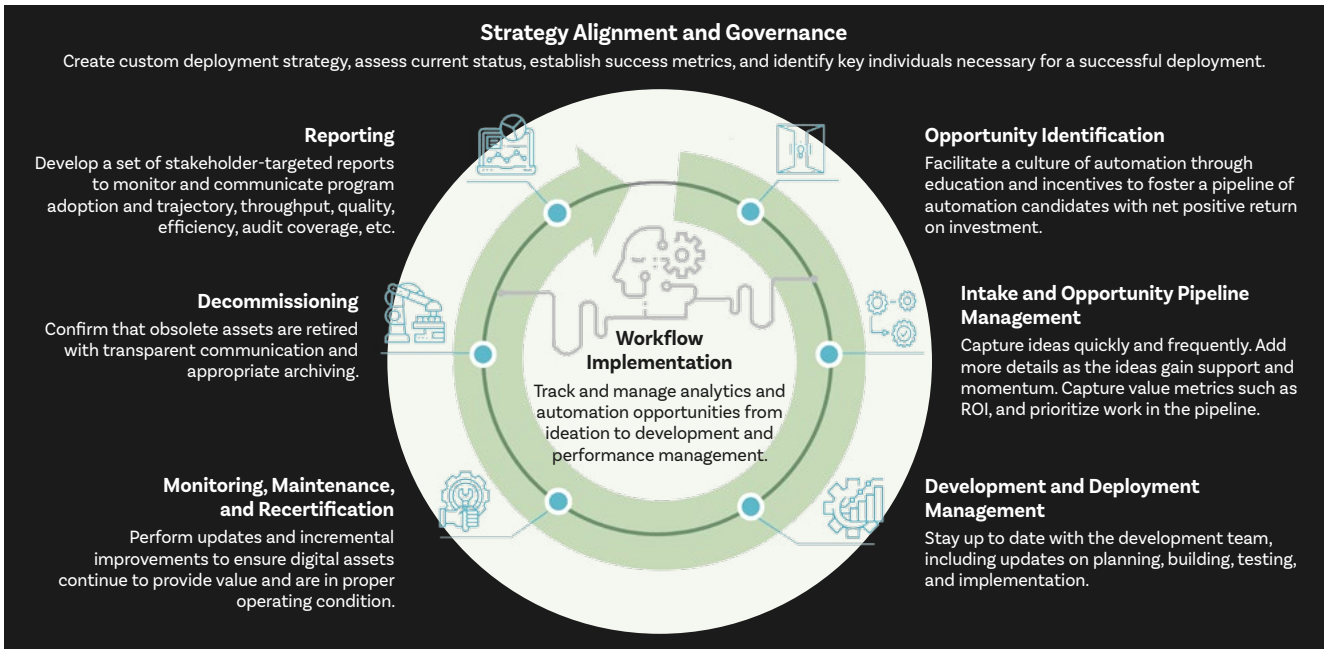


Additionally, IA's strategic vision should align with wider digital transformation initiatives underway across the organization. It's often preferable to leverage and reinforce the technology, training, and investments that the first and second lines of defense are undertaking. While objectivity and independence are part of IA's role, there are often opportunities to collaborate with other risk management functions without compromising independence. Leading organizations avoid reinventing the wheel by making the most of these relationships (for instance, by using a common risk taxonomy across the three lines of defense or by sharing development resources).

Digital Enablement in Action

Driven by a strategic vision, a mature, digitally enabled IA operating model should feature six key components that are connected by a workflow. See **figure 2**. While this list is not exhaustive, these components go a long way toward creating an environment that can address the most pressing goals for many IA organizations—namely, increasing risk coverage, reducing manual work, and producing data-driven insight.

Figure 2: Operating Model Overview



1. **Opportunity Identification.** Also known as demand generation, opportunity identification kicks off the overall automation process by creating a pipeline of automation ideas. Having a structured methodology (which enables auditors on the front lines to better identify automation opportunities) is fundamental to the long-term achievements of an IA modernization program. This methodology should be capable of identifying high-potential automation

opportunities—those that deliver strategic value as well as cost savings, while progressively advancing the digital maturity of the organization. The idea is to move the organization beyond the low-hanging fruit to scale automation across a variety of high-value use cases. The characteristics of such a methodology are detailed in the first part of this series, *Moving Internal Audit Deeper Into the Digital Age, Part 1: A Structured Methodology for Leveraging Automation to Modernize the Audit Function.*

Beyond the methodology itself, the tone at the top, training, and culture are also important. Auditors need to be trained in the opportunity identification process and be inspired to contribute new ideas. Additionally, they should have access to technical training and technology discovery workshops so they can become familiar with both standard technical tools and newer "disruptive technologies." Such training can help auditors make the leap from "I didn't know we could do that" to "we can use X, Y, and Z techniques to enhance testing and provide insight." Moreover, idea-generation labs and auditor automation challenges, where auditors can brainstorm and work collaboratively in a spirit of friendly competition, can help to foster an innovation mindset. Also, forums, newsletters, and other communication vehicles that tout individual and group progress can be useful in building momentum.

2. **Intake and Opportunity Pipeline Management.** As automation opportunities are identified, they should be captured and queued in a pipeline for evaluation by management. This enables IA to establish an inventory of viable automation opportunities that can be vetted for potential duplicates and ultimately ranked. Once opportunities are identified and queued, the business requirements should be fully built out. Auditors should document the business justification, test objectives, systems and data sources involved, and each audit-test step of the intended automation. From here, auditors should engage with lines of business and application management to confirm that all of the systems and data sources have been identified, ideally down to the levels of database, table, and field, if applicable. Including sample reports or backend data in the documentation for the automation opportunity can be instrumental to developers as they orient themselves to the requirements. For each opportunity, several attributes should be captured for use in assessing return on investment (ROI). An approach to assessing ROI is outlined in the first part of this series. Once the ROI for each automation opportunity has been determined, audit managers can readily identify those with the highest value potential and prioritize them for development.

Proper intake and pipeline management also helps the organization to align opportunities with available resources. In an environment where development resources are often scarce, care should be taken to confirm that the size and skillsets of the resource pool match the desired overall development timeline and the diverse technology requirements of the automations.

3. **Development and Deployment Management.** Once opportunities have been queued, vetted for value, fully built out in terms of requirements, and aligned to development resources, the next step is to develop and deploy the automated solution. Automation requires a range of specialty skillsets such as data wrangling, querying, modeling, scripting/coding, and visualizing. These specialists may reside within the IA function or they may be co-sourced from external vendors or from other parts of the organization, such as a centralized data analytics group or RPA center of excellence (CoE), which often sits under IT.

   One challenge to note when co-sourcing work internally, such as from an automation CoE, is that these teams often use their own ROI models to prioritize requests. With large revenue-producing and cost-saving initiatives routinely coming into CoEs from across the enterprise, projects that generate smaller returns may get lost in the shuffle. For instance, their ROI models may overlook the value of increased assurance, or fail to recognize a moderate reduction in manual testing hours. Because the metrics used by these groups are generally not tuned for risk and assurance activities, some IA shops prefer to use their own developers, supplemented by external partners as needed. This approach is often preferable to vying for CoE resources.

   Effective implementation of a digitally enabled IA operating model requires strong collaboration with development resources. Workflow tracking should be handed off to the developers during the development and deployment phase, and key milestones should be reported back in the form of status updates. This back and forth allows developers to use tools that are best for their team while keeping the workflow up to date. This phase of the lifecycle ends by moving the developed product into a production environment that protects the digital assets from unintended or unapproved changes.

4. **Monitoring, Maintenance, and Recertification.** Moving an automated solution or dynamic report into production may mark the end of the development and deployment phase, but further commitments will still need to be met. The automation will need to

be monitored by operations for proper execution. Exceptions will need to be addressed, which may require additional development to refine the automation. Auditors often request updates and enhancements due to changing business processes or data sources. These maintenance jobs should be prioritized in the workflow like new requests. Given the relatively high value-to-effort ratio for updates and enhancements, these requests can often be addressed quickly.

An effective digitally enabled IA operating model also prescribes periodic recertification of every digital asset in production. Recertification periods may vary based on the product type or other factors. Recertifications have two main components: 1) an attestation by an *auditor* that the digital asset provides business value, and 2) an attestation by a *developer* that the digital asset is performing as intended.

Without recertification, resources can be wasted. For instance, an automation could be checking user-access list attributes for an application that has been retired. Or, an algorithm could be running queries against a data warehouse that stopped receiving live feeds when a new data lake came online.

Auditors and developers have joint responsibility for recertification. An effective workflow has the ability to maintain the recertification calendar and assign tasks to specific auditors and developers.

5. **Decommissioning.** Due to insurmountable maintenance costs, failure to be recertified, or other factors, digital assets will eventually need to be retired. Decommissioning procedures confirm that these assets are taken offline for the right reasons, that communication about the changes is thorough, and all documentation and relevant history have been archived.

6. **Reporting.** The successful long-term management of a digitally enabled transformation program hinges upon meeting goals and anticipating upcoming needs. That is why reporting should be robust, combining input from auditors, business analysts, developers, and IA leaders. It should also be visually compelling and offer a dashboard or portal for leaders to review several layers of performance information. Some potential reporting metrics include:

Metric	Phase of Operating Model	Description
Automation program progress	Strategic vision	Assess all controls to determine those that have automation potential. Tag controls as: 1) to be reviewed for automation potential, 2) no automation potential found, and 3) has automation potential. Further tag the latter as either automation in progress or automation complete. Express the aforementioned tags as percentages of the total number of controls in order to measure the progress of the automation program against the initial and ongoing strategic goals.
Value	Strategic vision	Determine how the organization defines value (e.g., risk/control coverage, audit efficiency and effectiveness, coverage of audit assertions such as completeness, hours saved, etc.).
Cost	Strategic vision	Track the hours involved from ideation to deployment. While developers are automatically expected to track their hours, IA personnel should also track the time they spend on developing or researching ideas, defining requirements, creating documentation, and managing changes.
Intake and opportunity pipeline status	Intake and opportunity pipeline management	Report on the number of automation opportunities identified, the relevant business areas, and the auditors who are involved. Track the opportunities approved for development, their progress within the automation lifecycle, and opportunities waiting for assignment. Organize the opportunities by business area and technology required and identify the types of automations in the pipeline. Use the annual time-savings estimates, which are part of the overall ROI calculation, and compare to a current baseline.
Capacity	Intake and opportunity pipeline management Development and deployment management	Track automation opportunities in the pipeline that are pending requirements definition or associated documentation, identify what is causing the delay, and determine why they are unassigned. State how long the opportunity has been in the pipeline and assess its current state (i.e., percentage of completion). List developers without projects as well as those currently engaged and provide insight into what they are working on.
Prioritization	Intake and opportunity pipeline management	List the prioritization queue and provide the status of the opportunities in the queue.
Development	Development and deployment management	Compile all completed, in-progress, and pending automation opportunities. Add details around types of technologies involved, access requirements, and developers assigned.
Monitoring, maintenance, and recertification	Monitoring, maintenance, and recertification	Develop metrics to gauge automation performance, including the number of automation failures and fixes. Explore root causes of these issues. Develop metrics related to automation recertifications. As the automation program matures, resources will need to be allocated to address the increasing volume of ongoing recertifications.
Decommissioning	Decommissioning	Track how many automations are decommissioned in a given period. Examine the time between deployment and decommissioning to determine the average lifespan of an automation.

Reporting frequency, format, and associated level of detail should be tailored to the audience and support decision-making. Managers charged with running the automation program will require more granular detail, perhaps daily. Audit automation-program leadership will require more of an overview, perhaps monthly, to confirm the program is on track.

Workflow Design

Like the hub of a wheel, a structured workflow ties the six components above together into a cohesive cycle. An effective workflow tracks the automation lifecycle from opportunity identification to development and ultimately to decommissioning, and it is essential for scaling analytics and automation capabilities within IA. The workflow can be implemented using various applications, from spreadsheets or collaboration sites on the one end to custom-built systems or enterprise web platforms on the other. Ideally, the workflow system will have built-in reporting capabilities.

Regardless, the chosen workflow-enablement tool should give IA leaders the ability not only to track and monitor potential ideas and automation opportunities but also to review and approve them. There should also be a way to readily assign opportunities to developers who have the skills and the availability to develop the automated solutions. And, to close the loop, the tool should give IA leaders the ability to periodically review all of their digital assets and upgrade or decommission them as necessary.

A well-designed workflow is essential for unifying the overall process and holding all stakeholders accountable for their roles in the transformation. In addition, it accelerates automated solution deployment and provides the foundation from which to derive valuable process metrics. Such metrics include the number of ideas generated, prioritization lists, and anticipated ROI—not to mention development tracking, timing, and resource matching.

The Human Factor

Designing a digitally enabled IA operating model and developing automation and cognitive technologies is only half the story. The other half is auditors' ability to adapt to a different way of interacting with technology and information—and their capacity to think about the audit lifecycle and their role within it—in entirely new ways. For instance, automation and cognitive technologies can enable auditors to rethink their approaches to risk assessment and audit design while completely transforming fieldwork and reporting through full population testing and exception-based analytics. When approached with the relevant mindset, automation and cognitive technologies can provide increased accuracy, completeness, insight, and operational resilience by freeing auditors from mundane tasks so they can focus on analyzing and understanding risk.

However, effective adoption of a digitally enabled IA operating model depends largely on the organization's willingness to shift its culture. First and foremost, auditors should see cognitive and automation technology as a driver for positive change. Here, the tone is set from the top. IA leaders

should communicate the expectation that automation and cognitive technologies are permanent additions to the team that will increasingly enable IA's mission. They should also set strategic goals and communicate the vision for the organization, clearly defining a multiyear plan while providing adequate resources to support it.

Bottom-up engagement is equally important to the effectiveness of a digitally enabled IA operating model. Auditors should be incentivized not only to participate in the program but also to set high standards for planning and execution and to promote adoption of automation and cognitive technologies. Often, the incentives to use automation and cognitive technologies within an audit, and therefore take on extra risk, are misaligned with performance criteria, such as completing the audit on time and within budget. This misalignment can both discourage individual auditors and impair the overall program, since it sends mixed messages about the importance of digitally enabled transformation.

Conclusion

The three parts of this series collectively address how to move audit deeper into the digital age. More specifically, the first part examines how to leverage automation to modernize the IA function; the second part explores what IA needs to think about when auditing automation; and this third part, the final installment, offers a blueprint for scaling digital capabilities and transforming the audit lifecycle.

The three parts of the series share a common theme: ready or not, automation and cognitive technologies are here to stay. As such, these digital resources should be adequately governed and fully integrated into the operating model of the IA function. While the challenges of managing a digital workforce alongside a human one are significant, IA organizations that fail to incorporate these capabilities may be disrupted. Without the help of digital resources and talent, it is unlikely they will be able to keep up with the changing risk landscape and the evolving needs of the business.

As the velocity of change accelerates, the IA function has a fundamental choice: it can lead by embracing the future of work and showing other business functions how to develop and integrate digital resources, or it can follow and risk being left behind.

Automation takes many forms, delivers many benefits at FedEx

The word "automation" often evokes thoughts of end-to-end robotics process automation (RPA). But, automation and advanced analytics can take many forms, all of which can potentially add value. As Francisco Bertorini, Manager of Audit Analytics for Internal Audit (IA) at FedEx, explained, progressively building automation capabilities and generating user-centered value step by step is often the method for highly complex organizations such as FedEx.

Given that both audits and applications vary greatly across operating segments and regions, the audit analytics team at FedEx is not seeking to automate complex global scenarios. Instead, it is leveraging automation across three straightforward, high-value use cases that were identified via demos and feedback sessions with audit teams.

1) Risk-assessment dashboards: These tools employ task automation with key risk indicators (KRIs) embedded in the models to enhance the IA department's risk-profiling capabilities. As Francisco explained, the idea is to identify emerging risks so the audit team knows where to allocate audit resources. At the push of a button, auditors can use the dashboards to identify where risks are emerging (for instance, in operating segments, cost centers, or geographies).

2) Next-level deep dive: Once auditors have a sense of where risks are emerging, they need to know more about what is taking place. Using automation and analytics, this next-level solution helps the IA team perform a deeper dive into the initial risk profile so auditors can see anomalistic activity and better understand what is happening at a more detailed level.

3) Task automation: Task automation tools focus on giving auditors the capability to quickly perform common audit test steps, such as fuzzy matching or key control testing. This can help reduce the time needed to build a testing plan, since auditors can jump right in and perform testing within the tool itself (for instance, by having the capability to quickly isolate and review vendor invoices).

The FedEx IA department built out these digital capabilities and is now planning for future ones. The initial work focused on building an analytics team that primarily did ad hoc analytics consulting on a project-by-project basis. Over time, the department's analytics acumen increased and now the analytics team has begun pivoting to its next phase, which focuses on providing greater insight and foresight to the business through digital innovation.

The analytics team leapt into this phase faster than anticipated due to the pandemic. "After COVID-19 forced many of us to work remotely, we started leveraging Agile principles to collect user stories and assess the needs of our audit team members across the globe," Francisco commented. "Whether those needs pertain to risk assessments, audit planning, audit-script testing, or something else, we are creating transparency across IA by using Agile-based approaches to understand what our audit team members need. We then rationalize and prioritize those requests to get the most bang for our buck in developing tools with the highest return on investment."

Once the automation opportunities have been identified and prioritized, the analytics team goes to work, essentially acting as developers. Periodically, they report back to the end users, showing them what they have developed so far and then incorporating their feedback into the next iteration. "Agile enables us to approach analytics and auditing like application development," observed Francisco.

Implementing a progressive, digitally enabled IA operating model would not have been possible, however, without strong executive leadership. Francisco elaborated, "Our chief audit executive (CAE) has provided the vision for audit automation. Also, our company CEO and chairman established three operating principles, one of which is to innovate digitally and bring automation to the way we work." This strong tone at the top has allowed the IA department to lay the foundation for robust analytical and digital capabilities, and it has also enabled the analytics team to leverage the enterprise's overarching cloud financials and analytics package. "By leaning into the enterprise data strategy and analytics applications, there are no licensing or technology costs for our audit analytics program—zero," said Francisco. "And, since we don't have to focus on the data management piece, we can spend more time in user-centered design thinking, which allows us to deliver speed to value at scale."

In communicating the value of this digital approach to the board and audit committee, Francisco explained that the CAE emphasizes the enhanced quality and effectiveness of the audits as well as the efficiencies gained in various phases of the audit lifecycle. He elaborated that IA may not be able to pinpoint the types of issues they do without using automation and advanced analytics. Thus, risk identification is essential to the value equation, along with the department's commitment to being trusted business advisors. "When presenting our stakeholders with audit findings and corrective action plans, it is about focusing on solutions that make a positive impact to the business, and I think we're doing a phenomenal job of leveraging technology to deliver insight and foresight," emphasized Francisco.

We expect the future state of the analytics program at FedEx will likely focus on gaining even greater efficiencies. Remote auditing has prompted the IA function to think differently about automation, particularly how they can tap into the various data sources that exist at FedEx. "We are working to develop an arsenal of analytics that give us the information we need without having to disrupt our audit stakeholders—in other words, our goal is to make planning, fieldwork, and reporting as efficient as possible for the end user," he concluded.

Contacts

Neil White
Principal
Deloitte & Touche LLP
nwhite@deloitte.com

Michael Schor
Partner
Deloitte & Touche LLP
mschor@deloitte.com

Martin Rogulja
Senior Manager
Deloitte & Touche LLP
mrogulja@deloitte.com

Contributors

Ben Horton
Senior Manager
Deloitte & Touche LLP
behorton@deloitte.com

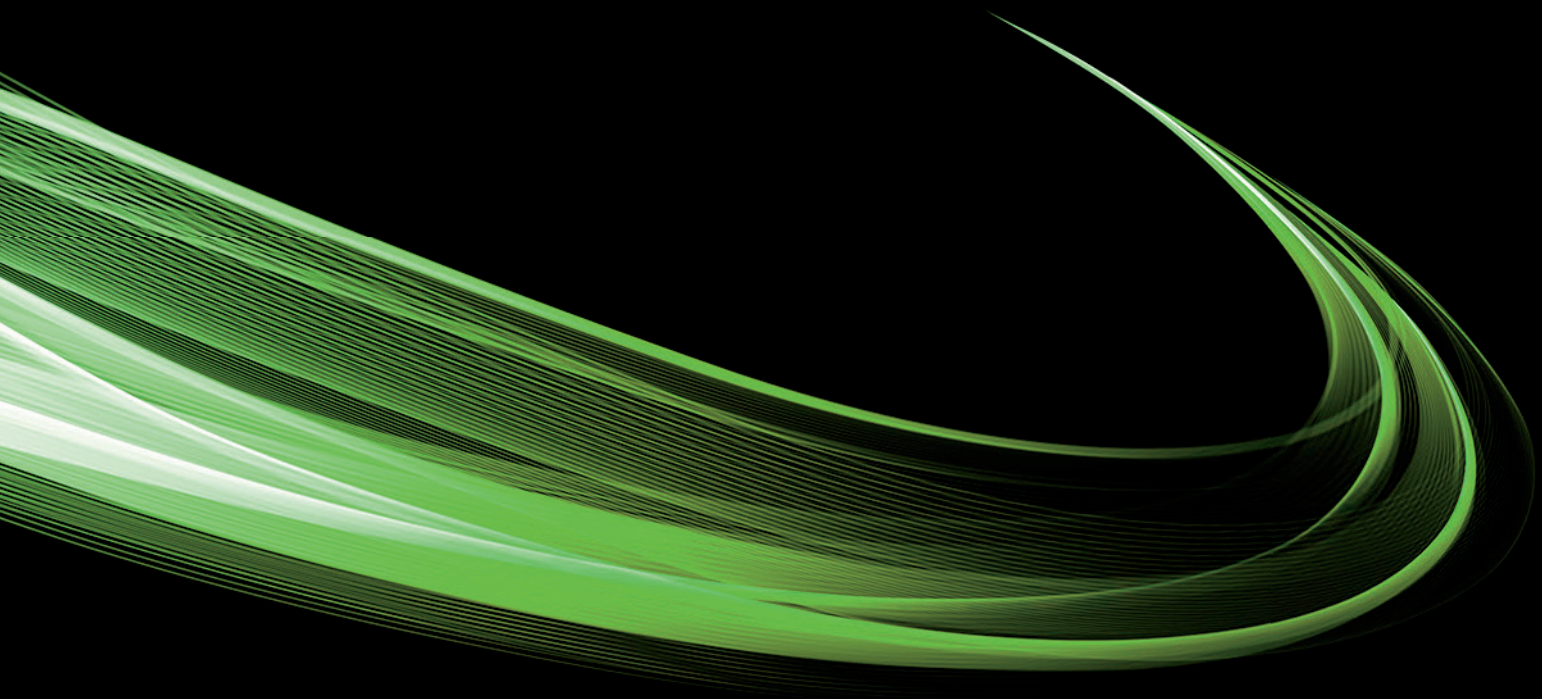
Patrick Girling
Manager
Deloitte & Touche LLP
pgirling@deloitte.com

Asef Qayyum
Senior Consultant
Deloitte & Touche LLP
aqayyum@deloitte.com

2020-1764

Moving Internal Audit Deeper Into the Digital Age: **Part 1**

A Structured Methodology for Leveraging Automation to Modernize the Internal Audit Function



INTERNAL AUDIT FOUNDATION™

Deloitte.

Published by the Internal Audit Foundation
1035 Greenwood Blvd., Suite 401
Lake Mary, Florida 32746, USA

The IIA's International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The IIA and the Foundation work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today's business world. Much of the content presented in their final reports is a result of Foundation-funded research and prepared as a service to the Foundation and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or the Foundation.

ISBN-13: 978-1-63454-070-4
23 22 21 20 19 1 2 3 4 5

Contents

Moving Internal Audit Deeper Into the Digital Age

A Structured Methodology for Leveraging Automation to Modernize the Internal Audit Function

Robotic process automation (RPA) is among the most prominent disruptive technologies on the market. As early adopters demonstrate its ability to modernize and digitize business functions, internal audit (IA) departments increasingly recognize the automation's potential for improving audit coverage, speeding process execution, and freeing resources from routine tasks so they can focus on strategic, value-generating activities. Some IA organizations have automation plans and are well on their way toward executing them, while others are still contemplating how to embed RPA into their IA functions. In either case, now is the time for IA departments to accelerate their progress. With both budget constraints and an expanding and diversifying risk landscape, the call for thoughtful, progressive deployment of RPA within IA is intensifying.

The first step in effectively leveraging automation to modernize internal audit is to obtain a thorough understanding of what RPA is, what it isn't, and the benefits it can provide. Having a solid grasp of the technology's capabilities and constraints can increase the chances of obtaining a return on investment and utilizing the tools to their full capacity. The next step is to adopt a systematic, analytics-driven methodology for identifying and prioritizing high-potential opportunities for IA automation. A structured approach is essential for charting a course toward continuous improvement and value realization once the readily apparent opportunities for RPA have been exploited. Underpinning these actions, it is also important for senior management to express a long-term commitment to RPA.

What RPA Is

RPA platforms, or "software robots," perform routine business processes by mimicking the way that people interact with computer systems. Just as users know where to click to control applications and manipulate data, software robots can be programmed to take similar actions. A single task or an entire end-to-end process across different applications and platforms can be executed by a single software robot with very little human intervention, typically only to manage exceptions.

RPA is best suited for processes with repeatable, predictable interactions with software applications. These processes typically lack the scale or value to warrant IT transformation through deployment of a new platform. Indeed, the beauty of software robots, or "bots" for short, lies in their simplicity: they are typically low cost and easy to implement. Via straightforward programming that requires minimal or no code, bots can enhance process efficiency and service effectiveness without necessitating fundamental process redesign that is often associated with big-system-based automations. Inherently vast, potential RPA scenarios range from generating responses to validating data across multiple systems to fully automating an end-to-end process.

What RPA Isn't

RPA is not machine learning (ML) or artificial intelligence (AI), which are self-teaching and to some degree replicate human perception and judgment. RPA does not attempt to read, interpret, or think. Governed by business logic and structured inputs, software bots can be programmed to perform routine jobs in an enterprise resource planning (ERP) system, such as processing transactions, manipulating data, triggering responses, and communicating with other systems. In the traditional sense, they can eliminate the need for users to click and calculate but not for them to analyze and strategize. That said, some companies are beginning to enhance their RPA platform capabilities by injecting them with cognitive capabilities, such as ML, speech recognition, and natural language processing. Already, there are many AI-enhanced bots in production that read emails, classify the content and respond automatically, make phone calls to alert users to failures or exceptions that need attention, and use optical scanning to go to websites and scrape off information for further processing. If this trend continues, the lines between advanced digital technologies will increasingly blur.

Potential Benefits of RPA in IA

In terms of the potential benefits of RPA, increased process speed, reduced errors and costs, and streamlined processes obviously stand out. But, in addition to the ability to perform the same audits faster and more effectively, there are many other reasons that an IA organization may choose to pursue automation. Deloitte UK's annual Global Robotics Survey sheds light on some of them. In the 2017 report, responding shared services and other administrative organizations indicated that RPA continues to meet and exceed expectations across multiple dimensions, including improved compliance (92%), improved quality/accuracy (90%), improved productivity (86%), and cost reduction (59%).

IA organizations can potentially benefit from all of these dimensions and more. RPA can help to standardize audit processes, which reduces manual errors and enhances audit quality. It is also highly traceable, which can allow errors to be detected more readily and rectified more easily. Often, productivity and talent retention are simultaneously enhanced as full-time employees (FTEs), are freed from performing repetitive tasks, and redirected toward more rewarding work. Tasks such as engaging with business leaders on strategic risks, joining risk committees, and participating in the governance and oversight of major capital projects, all in all helping the function to focus on the truly greatest risks, are just a few of the productive ways employees can spend their newfound time.

Common Situations for Applying RPA

- Gathering background information and metrics from multiple systems or sources to better define audit scope
- Continuously monitoring business operations that would be too demanding and/or expensive if done manually
- Pre-populating documentation requests based on audit scope
- Generating planning documentation by automating text-heavy documents
- Performing "what if" analysis on more data more frequently
- Detecting suspicious logs associated with IT systems
- Real-time reporting of frauds arising in financial systems
- Testing control effectiveness based on a sample or the entire population

By enabling full-population testing, as opposed to statistical sampling, RPA can enhance compliance and risk management, thus strengthening the second line of defense. For example, RPA can test the full population of foreign transactions to identify those occurring in countries sanctioned by the Office of Foreign Assets Control (OFAC) or to flag accounts with improper financial controls. This ability to carry out full-population checks across business units can enhance IA's ability to identify regulatory and reputational risks and provide a greater level of assurance regarding the effectiveness of a company's financial and technical controls. Furthermore, by using risk analytics and data visualization tools in conjunction with RPA, auditors can gain greater insight into business processes, allowing them to perform more focused audits while still testing 100 percent of the population.

As an organization's audit capabilities mature, even more benefits may be generated. For instance, RPA can enable IA to test more frequently, with some organizations already transitioning to a continuous auditing model for providing more timely insights to the business. Opportunities for combining data from inside and outside the company can add new richness to insights and provide a more granular understanding of risk. And, RPA-enabled benchmarking, comparative analysis, and trending can be used to enhance on-the-job learning and development while delivering more powerful results to business stakeholders.

Ultimately, progressive RPA deployments that build upon and enrich existing analytics technologies can aid the IA organization in developing a culture of digital adoption and continuous innovation. Such a culture can create a virtuous cycle of ongoing improvement by applying next-gen technologies and data-science disciplines to the audit process.

The Need for a Structured Approach

Despite the long list of potential benefits, discernment is necessary in determining where to apply RPA for maximum effect. While there are certain situations where RPA works well, there are also situations where it does not. Automation is **NOT** appropriate for processes that:

- Involve complex interactions
  - Example: A process that involves a non-standardized method of obtaining data or answers
- Require a judgment call
  - Example: The review that is required when an invoice exceeds a monetary threshold
- Entail high-level cognitive tasks
  - Example: Pattern recognition in determining data clusters and predictive models

Using the general guideline of "repetitive and rule-based," IA organizations can usually find some low-hanging fruit. After that, however, the process of identifying and prioritizing opportunities for automation becomes more complicated. Sole reliance upon finite metrics, such as cost to implement and time saved, can cause added-value automation opportunities—such as those that improve risk mitigation, human-resource allocation, and talent management—to be overlooked. Often what is needed, instead, is a structured methodology for identifying high-potential automation opportunities that deliver strategic value as well as cost savings, while progressively advancing the digital maturity of the organization. It is imperative to understand the value that automation of standardized processes will bring and perform objective assessment of complexity vs. benefits of the automation. To this end, for example, Deloitte has developed an eight-step methodology aimed at helping IA organizations not only to identify appropriate opportunities for RPA but also to develop an automation road map and position themselves to drive value from it.

The Methodology

Step 1: Screen Opportunities

The first step involves reviewing the current state of the IA organization to understand where and how RPA can be embedded to increase audit coverage and improve efficiency and effectiveness. This typically consists of:

- Examining the audit plan to gain a contextual understanding of the business environment and key activities
- Identifying:
    - Processes that are standardized and rule-based, as opposed to variable and decision-based (e.g., analysis and recommendations)
    - Tests, or parts thereof, that are rule-based and can be performed by analyzing and comparing large datasets
    - Controls where full-population testing would be feasible and beneficial
    - Tests that could benefit from increased scope

Output: A list of tests and specific controls that could potentially be automated.

Step 2: Assess Value

Once a list of potential candidates for automation has been compiled, the next step is to assess the potential value of each according to key criteria, typically related to: time and monetary savings, inherent risk to process, productivity improvements, customer and employee satisfaction, and risk-mitigation impact. The ultimate objective is to score the candidate processes according to their total value potential. This includes both quantitative and qualitative benefits, evaluating them on their ability to enhance effectiveness, ease, and quality, in addition to efficiency by assessing benefits through low, medium, and high tiers.

Output: A comparison of candidate processes according to their potential business value (see **figure 1**).

Figure 1: Key Outcome: Each of the Candidate Processes Can Be Compared by Their Relative Complexity and Business Value

Criteria #	Key Criteria	Low Value	Medium Value	High Value	Definition
B1	FTE capacity improvement	<1 FTE	1-10 FTE	>10 FTE	How many FTEs are currently assigned to the process?
B2	Decreased process handling times	<10%	10-90%	>90%	How much deduction in process handling time will RPA offer?
B3	Increased accuracy, quality, and risk reduction	No significant impact	10-20% increase in compliance targets	>20% increase in compliance targets	What is the risk level involved and are there any quality issues in the current process? If so, will RPA increase compliance targets by reducing risky steps?
B4	Reduction in customer wait times	<10%	10-90%	>90%	What is the reduction in wait time experienced by a customer as a result of automating this process?
B5	Improvement in customer interactions	No improvement	Slightly improved	Optimize customer service	How will RPA improve the customer service processes via simplifying the process and/or by integrating customer channels, business data, and enterprise applications?
B6	Removal of repetitive tasks/ value-add enhancement	No impact	Removal of select repetitive tasks	Complete removal of repetitive tasks	How well does RPA remove the repetitive tasks for the user? Does the opportunity exist to upskill the workforce in more value-added tasks and reduce attrition rates?
B7	Reusable components	No existing reusable components	A couple of modules with significant adjustments needed	A lot of modules with minor adjustments needed	Does the potential exist to introduce an agile capability to respond to ever-changing business processes by being able to reuse components? If so, then this criteria has a high business value and the ability to ramp up the workforce as required.
B8	Replication of processes/ tasks across business units and geographies	No replication applicable	N/A	Some replication applicable	If the process today is performed by a team that is widely distributed geographically—and for each of the team members the process is only a fraction of their work—some process transformation initiative, with the objective to centralize the process, may be necessary before embarking on the automation journey.

Source: Adapted from "RPA Opportunity Assessment Framework," Deloitte Australia 2018, p. 11.

Step 3: Evaluate Complexity

After performing a value assessment, the focus then turns to determining the feasibility of automating the candidate processes. One way to assess feasibility is to evaluate process complexity against key criteria, such as the number of applications involved, duration, data handling, access security, and geographic scope. Similar to the aforementioned value assessment, the goal of the complexity assessment is to score the candidate processes according to their degree of automation difficulty (i.e., complexity), parsing them into low, medium, and high tiers.

Output: A comparison of candidate processes according to automation feasibility (see **figure 2**).

Figure 2: RPA Opportunity Assessment Framework

Criteria #	Key Criteria	Low Complexity	Medium Complexity	High Complexity	Definition
C1	Number of applications	<3	=3	>4	How many programs does the process touch?
C2	Number of screens	<10	10-30	>30	Within a particular application, how many different panes/pages does the process interact with?
C3	Number of actions	<20	20-50	>50	How many times is an operation executed on the screen (i.e., copy/paste data, open/close an application, download/upload an attachment, create/delete row in a spreadsheet, log on/off, etc.)?
C4	Scale of exception handling expected	Low	Medium	High	To what degree does the process predictably deviate from the norm? And what is the complexity of the steps to handle this deviation?
C5	Data type	Digital, structured, and standardized	Digital, structured, and standardized	Digital, structured, and unstandardized	Structured – emails with templates, Excel spreadsheets, etc. Unstructured – emails of plain text, PDF documents, etc.
C6	Data handling required	Copy/paste	Copy, paste, read, and modify data	Copy, paste, read data, data enrichment, PDF data extraction	What is the nature of the interactions with the screen listed above? Copy/paste, read and modify, data enrichment, or data extraction?
C7	Access security	Single Sign-On (SSO)	Application-managed credentials	Authentication structure not documented or maintained	Type of security infrastructure and number of touch points that require clearance/authentication.
C8	Process geography	Local process	Multi-location process requiring adaptation to code (e.g., GIAC Security Essentials Certification)	Global process with multiple variations and code adaptation requirement	How many physical machines does the process use and where are they located? Consider difference in salaries across geographies for weighting.
C9	Process redesign required?	No process changes required	Minor process changes required (1-3 steps not satisfied)	Significant process redesign required (4-8 steps not satisfied)	Does any step in the process need to be changed to make it RPA eligible? Is there any human judgment required?
C10	Associated level of operational risk	Non-core processing	Time or business-dependent processing	Business critical BAU processing	Business impact if the process were to stop. Consider financial risks, chance of robot making a mistake, meeting SLA requirements, etc.
C11	Typical duration	4-6 weeks	7-9 weeks	12-14 weeks	Development time to productionize.

Source: Adapted from "RPA Opportunity Assessment Framework," Deloitte Australia 2018, p. 10.

Step 4: Qualify Processes

Once business value and complexity have been determined, the processes can be mapped onto a selection matrix or scorecard, with the categories of automate now, road map priority, automation opportunity, and automation challenge.

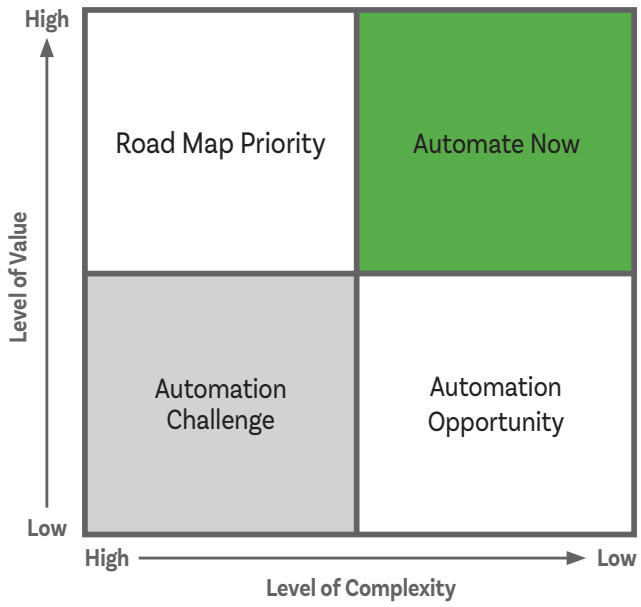
Once the processes have been assigned to the various quadrants on the matrix, IA leaders can consult with process owners to:

- Validate the value and complexity findings.
- Prioritize processes with immediate automation opportunities based on value and complexity metrics.
- Understand the full end-to-end process, which will ultimately guide the creation of automation documentation.
- Comprehend the level of cooperation from stakeholders, data owners, and other members of the business.

Informed by the scorecard and subsequent discussions with process owners, IA leaders can determine which processes warrant immediate or near-term action, which ones can wait, and whether or not some processes are worth automating at all.

Output: A prioritized list of processes to automate (see **figure 3**).

Figure 3: RPA Process Selection Matrix



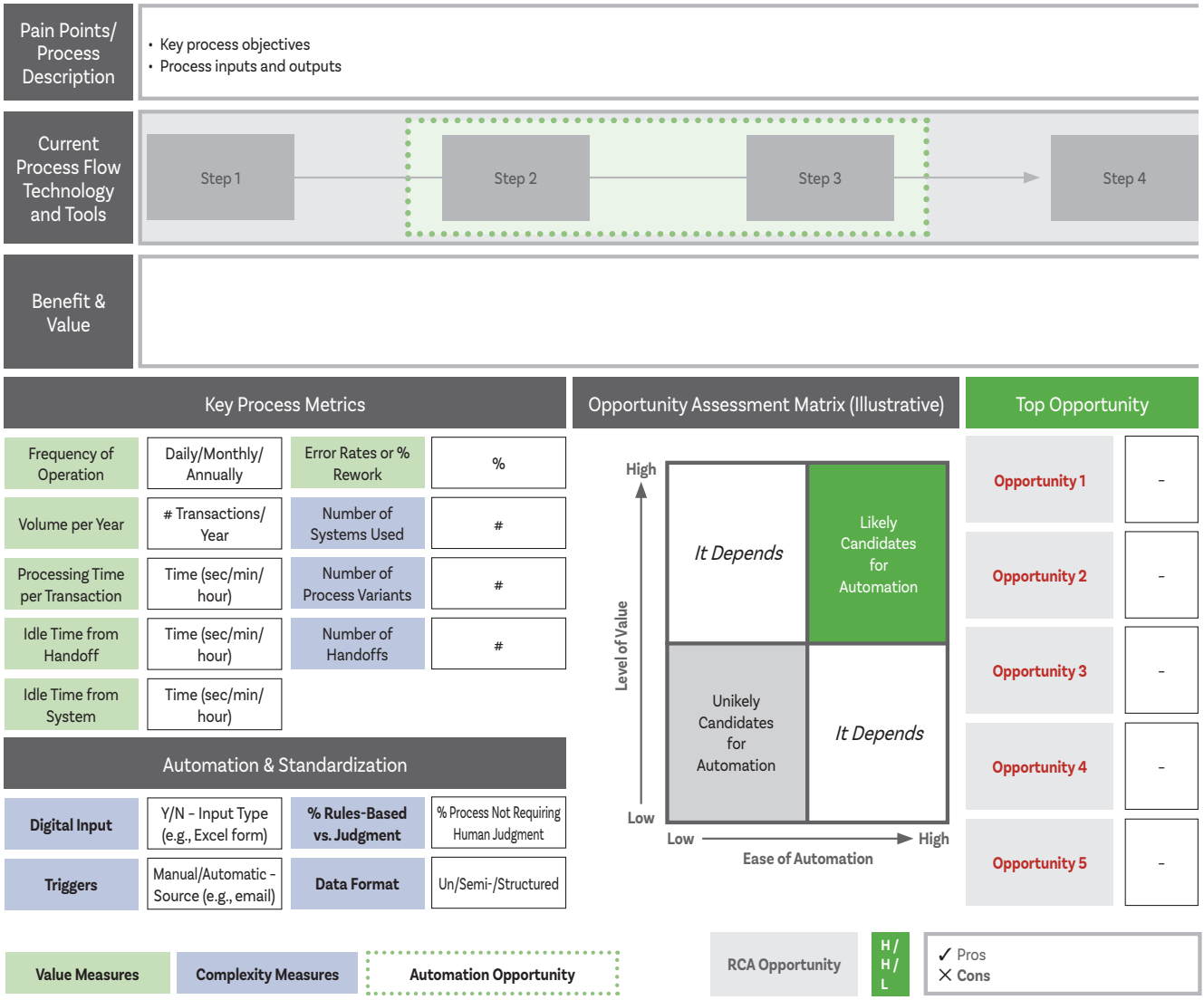
Source:

Step 5: Create Process Qualification Document(s)

A process qualification document (PQD) is a framework for presenting important information about a specific process at a high level. It illustrates and describes the process flow, explains challenges and required improvements, summarizes the business case, and organizes contact and ownership information. A PQD should be created for each process deemed an automation priority. The purpose of the PQD is to facilitate discussion with management in preparation for obtaining approval and funding.

Output: One PQD per priority process (see **figure 4**).

Figure 4: Sample Process Qualification Document



Step 6: Review and Signoff

It is important for IA and IT to agree that each PQD accurately captures the process to be automated, and an official document is essential for codifying this agreement. A leading-practice signoff document should typically include at a minimum:

1. A list of identified processes suitable for automation
2. The corresponding PQD and selection matrix for each

After final agreement has been reached among IA, IT, and the automation development team, the design phase can begin.

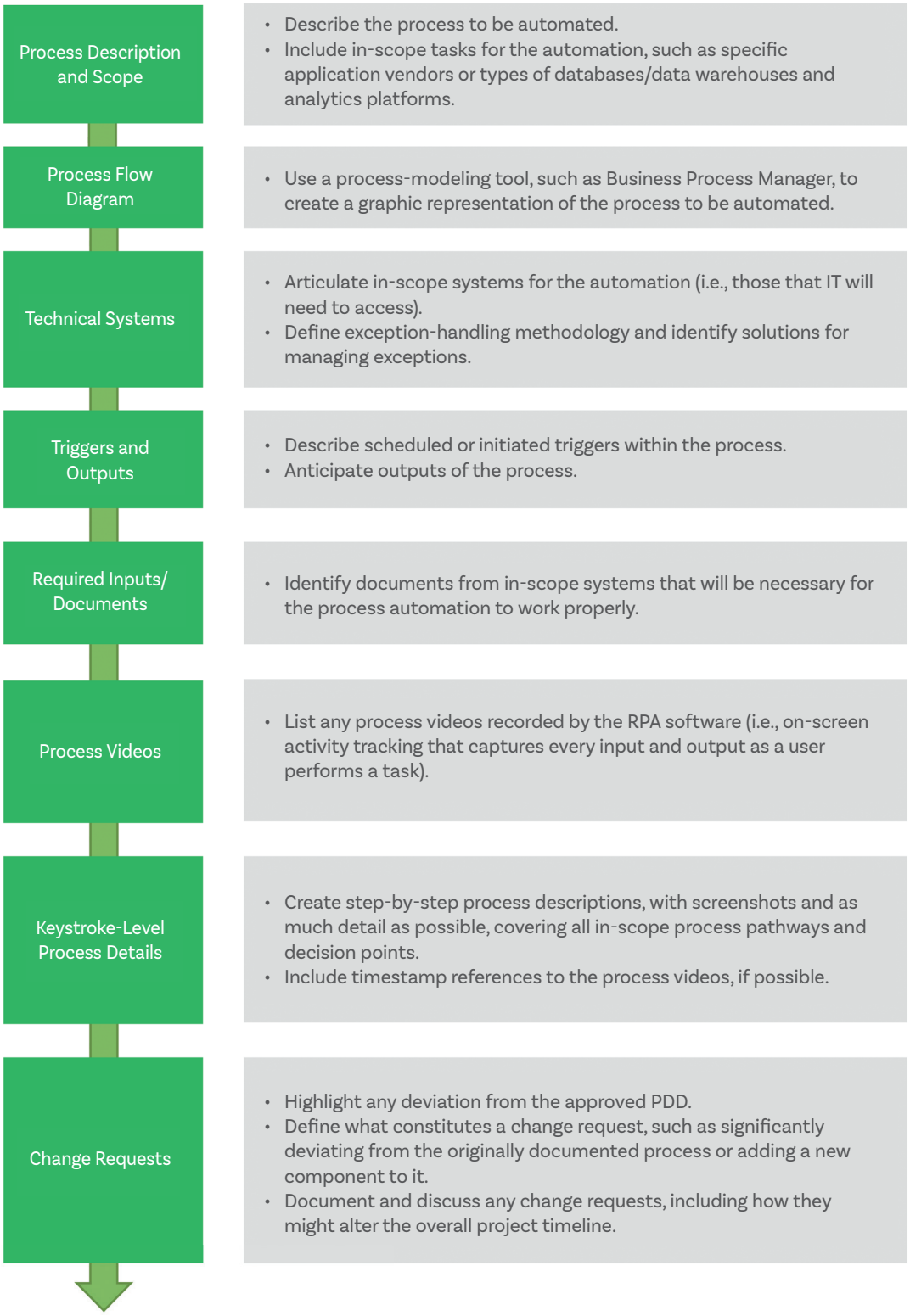
Output: Signed document approving the processes to be automated.

Step 7: Produce Process Design Document(s)

The process design document (PDD) provides an overall framework for automation development. It includes a scope description, a step-by-step process flow, technical descriptions, required inputs and documents, and change requests. A leading-practice PDD, as detailed in **figure 5**, includes key-stroke-level details and matching screen shots so the developer can experience the process firsthand. The PDD not only guides development, but also facilitates discussion about the impact of change requests upon the process flow and project timeline.

Output: One PDD per prioritized process.

Figure 5: Sample Process Design Document



Step 8: Establish an Internal Audit Specific Automation PMO Group

An automation project management group (PMO) can lead IA in its efforts to scale RPA by leveraging common technology, a centralized governance model, and standard processes and procedures. It typically comprises several cross-functional roles that collectively oversee current and future automation within a business unit or across the whole organization:

- Automation sponsor: Owns the RPA initiative and participates in executive RPA meetings
- Automation PMO leader: Manages the RPA PMO group within IA, defines the RPA strategy, and acts as the IA RPA evangelist
- RPA change manager: Serves as the RPA change agent across the enterprise; creates and executes the change and communication plan
- Automation solution architect: Defines the architecture and serves as the guardian of the automation solution from end to end.

Skills commonly found in an automation PMO group include strategy, process reengineering, IT infrastructure and development, change management, and customer support. As organizations scale, all of these skills are necessary for choosing a fit-for-purpose operating model and determining an appropriate level of centralized governance. Automation capability maturity, available resources, and tools leveraged across business units are frequently important factors in making these decisions. In addition, the IA PMO group provides input and acts as subject matter experts (SMEs) in creating a risk and control framework for auditing business RPA-driven processes.

While the size of some IA departments may warrant the creation of an IA specific PMO group, smaller IA groups might need to leverage knowledge and technical expertise found within business and IT groups. However, it is important to have designated resources that will drive the implementation of the automation across IA and build the relationships across the organization.

Value Realization

Software bots can be programmed to automatically execute repetitive processes and process large quantities of data, but they can't be programmed to automatically generate value. Making the bots work in a way that produces the intended results requires an operating model that fosters cross-functional relationships by:

- Bringing IT on board early to help establish automation criteria and determine if it would be worthwhile to automate a given task
- Training auditors and IT professionals so that both groups understand the automation criteria and how automation tools can be applied
- Encouraging an open environment for sharing knowledge and exchanging ideas among the PMO and IT and audit teams

RPA Gets Smarter

The power of automation can be significantly enhanced by deploying RPA in conjunction with cognitive technologies, such as natural language generation, natural language processing, ML, and computer vision.

For instance, RPA infused with ML capabilities can determine why an invoice or a transaction had been classified as fraud in the past and then look for those clues in new samples. If a match is found, it can be flagged as needing further inquiry.

Computer vision, which enables automation tools to recognize text and items within remote desktops, extends these capabilities deeper into the enterprise. For example, with the help of computer vision, ML can extract information from new, remotely created documents, such as invoices or bills of sale. For instance, once the tool learns to extract critical information from one type of document, it can extract it from other types by looking for "key context" descriptors, such as total price or tax.

Conclusion

When deployed successfully, RPA can significantly reduce and—in some cases—eliminate the need for human intervention in performing low-value, mandatory audit testing. This, in turn, can save hundreds of person-hours that can be redirected to higher-value activities. Second-line-of-defense functions, such as compliance, may also benefit from using RPA to reduce repetitive or redundant monitoring activities.

These possibilities are just the beginning. RPA that has been enhanced with ML and AI can tackle higher-level audit activities that have traditionally required human judgment, such as transaction classification, exception-based testing, and analytical dashboards. By allowing IA professionals to spend even more time on strategic activities, advanced RPA can promote greater collaboration among the three lines of defense, with the ultimate goal of enabling an integrated approach to risk management.

By implementing an operating model where audit and IT can work together to identify and develop high-potential opportunities, IA organizations have a better chance of reaping these and other intended benefits from automation. Some leading-practice organizations are discovering that the imperative is not only to automate but also to take advantage of the resources saved by redirecting them toward ongoing modernization and continuous improvement. Here, the human element can't be ignored. Bots may have the muscle to process huge amounts of data and find patterns and exceptions, but only people have the brains to decide what matters most.

Contacts

Michael Schor
Partner
Deloitte & Touche LLP
mschor@deloitte.com

Neil White
Principal
Deloitte & Touche LLP
nwhite@deloitte.com

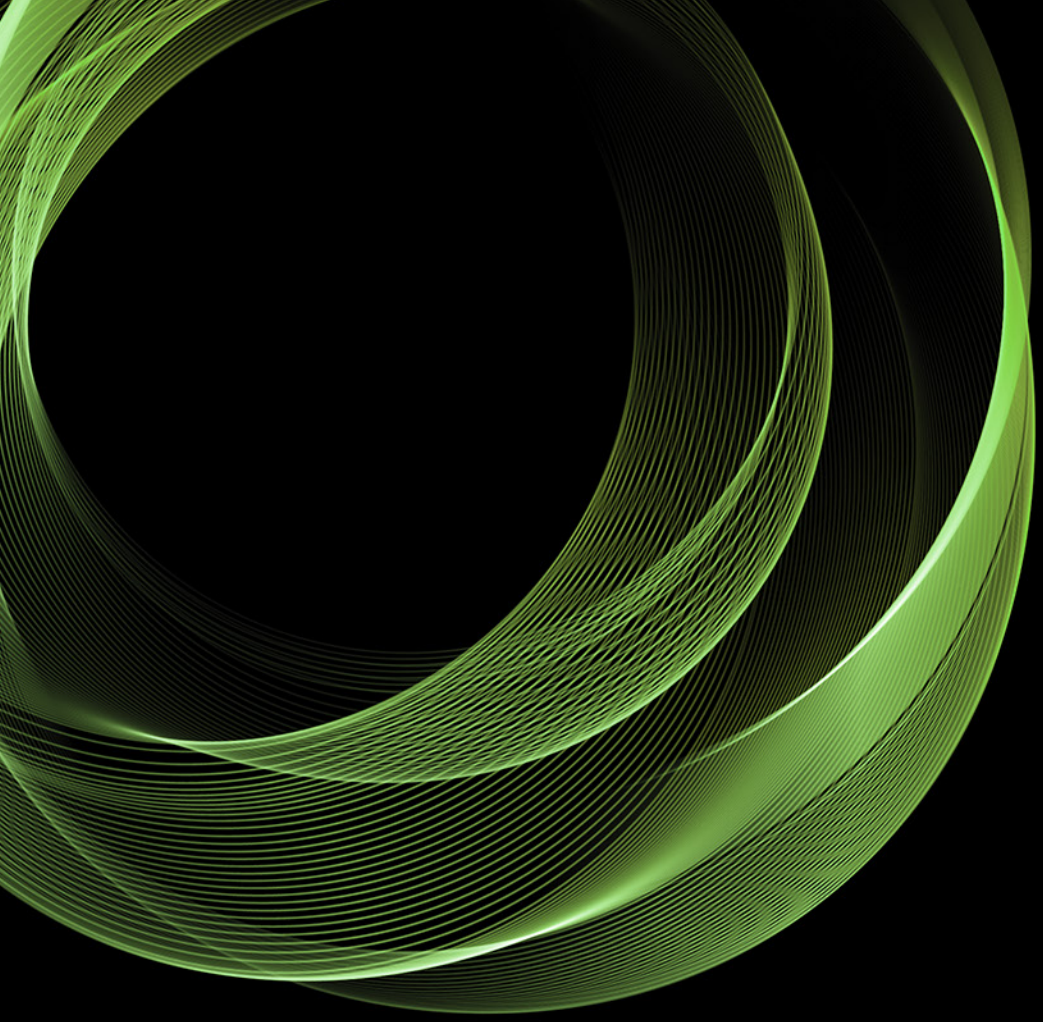
Martin Rogulja
Senior Manager
Deloitte & Touche LLP
mrogulja@deloitte.com

Contributors

Kevin Kurtz
Consultant
Deloitte & Touche LLP
kekurtz@deloitte.com

Asef Qayyum
Consultant
Deloitte & Touche LLP
aqayyum@deloitte.com

2019-356



Moving Internal Audit Deeper Into the Digital Age: **Part 2**

What Internal Audit Needs to Think About When Auditing Automation

INTERNAL AUDIT FOUNDATION™

Deloitte.

Published by the Internal Audit Foundation
1035 Greenwood Blvd., Suite 149
Lake Mary, Florida 32746, USA

The IIA's International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The IIA and the Foundation work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today's business world. Much of the content presented in their final reports is a result of Foundation-funded research and prepared as a service to the Foundation and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or the Foundation.

ISBN-13: 978-1-63454-076-6
24 23 22 21 20 1 2 3 4 5 6

Contents

Moving Internal Audit Deeper Into the Digital Age

What Internal Audit Needs to Think About When Auditing Automation

When modern automation tools enter an organization, they do not arrive alone. They bring with them a number of new risks. As discussed in the first part of this series, automation and cognitive technologies can potentially go a long way toward improving organizational responsiveness, speeding process execution, increasing process accuracy, lowering costs, and freeing workers from routine tasks so they can focus on strategic, value-generating activities. While modern automation tools can replicate many of the tasks traditionally carried out by humans, they simultaneously raise the bar on what is required of the people who must work alongside them.

As automation expands, traditional people skills such as critical thinking, creativity, and problem-solving are becoming more important than ever. While some organizations are focused on the "nuts and bolts" of automating existing processes, those further along the maturity curve are starting to restructure talent management and the nature of work itself so that both humans and machines can create more value. This often includes organizing work and processes more effectively, acquiring new skills, and redefining careers. Internal audit (IA) is not immune to these shifts. At the very least, IA needs tech-savvy employees who understand the new risks posed by automation and how to audit those risks. Beyond that, IA has a new imperative: auditors need to know digital since they live and work in a digital world.

Automation Risk Framework – the Mandate for Good Governance

Imagine the following scenario. Development teams within multiple business units work to develop bots, some in critical or regulated areas. Meanwhile, the department heads disagree on who owns automation support. The bots are deployed but a problem arises with one of them that prevents the export of important operational data. Nobody knows who to call to troubleshoot the issue, let alone how to prevent this programming bug from halting the downstream systems that need this data to function properly. Compliance is also jeopardized, since the data is additionally required for environmental, health, and safety reporting. With these bots in production, the errors

compound quickly, forcing the company to undertake a costly and messy "forensic fix."

As this example illustrates, the risk and control landscape for automation is highly complex, extending well beyond information technology (IT) risk. Although IA departments are accustomed to complex environments and to working with established risk-management frameworks, automation changes the game by adding new categories to these frameworks, along with introducing new risks into existing groupings. With this in mind, Deloitte has developed an expanded framework for classifying the key risks associated with automation (see **figure 1**):

1. Operational Risk — Processing errors may be magnified, concentration risk may be created, and disaster recovery could be made more difficult.

2. Financial Risk — Errors can result in financial or reputational losses, program return on investment (ROI) may not be met, and increased automation may have tax implications.

3. Organizational Risk — Human process intervention could be made difficult, training and development may fall behind the pace of technology, and maintaining specialized talent levels may be challenging.

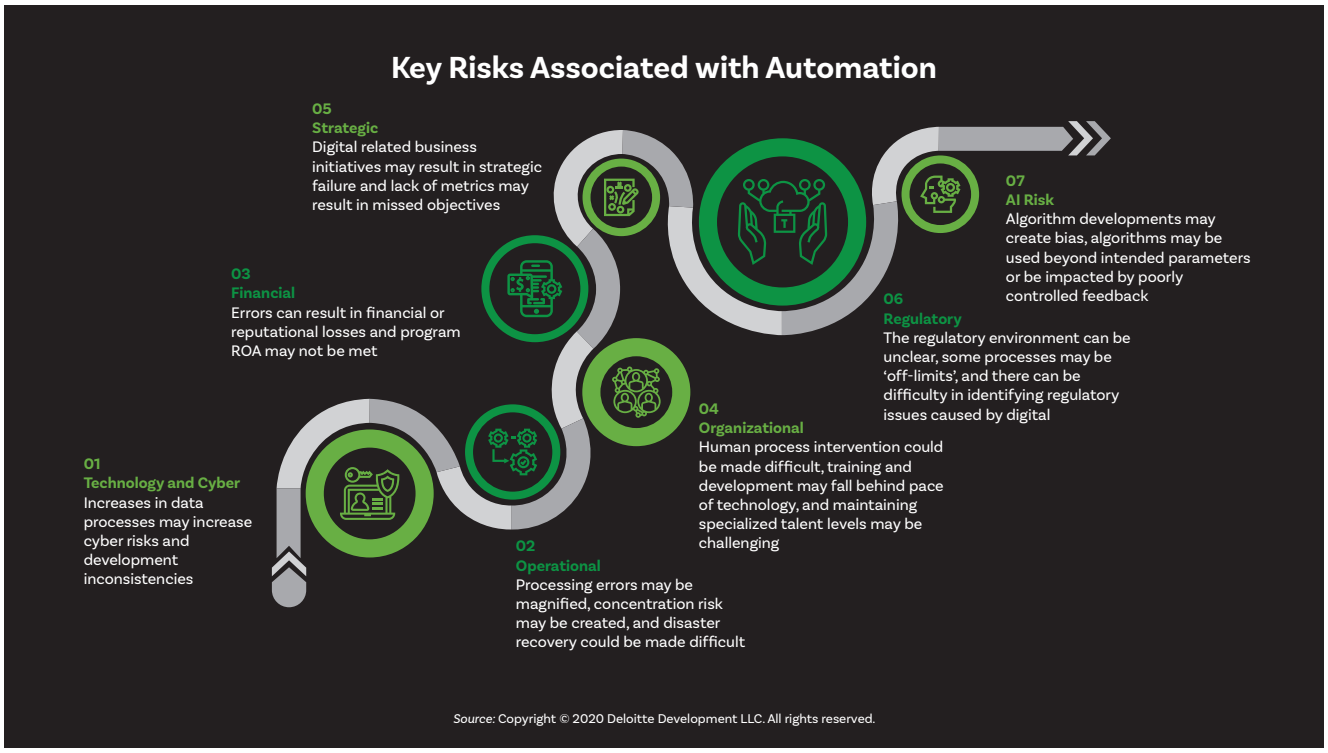
4. Strategic Risk — Automation-related business initiatives may lead to strategic failure and lack of metrics may result in missed objectives.

5. Regulatory Risk — The regulatory environment can be unclear, some processes may be "off-limits," and it can be difficult to identify regulatory issues caused by automation and cognitive technologies.

6. Technology and Cyber Risk — Automation technology that enables high-speed, high-volume data processing exposes organizations to cyber risks that might not be accounted for. It also requires thorough planning to identify and address potential impacts to existing IT infrastructure.

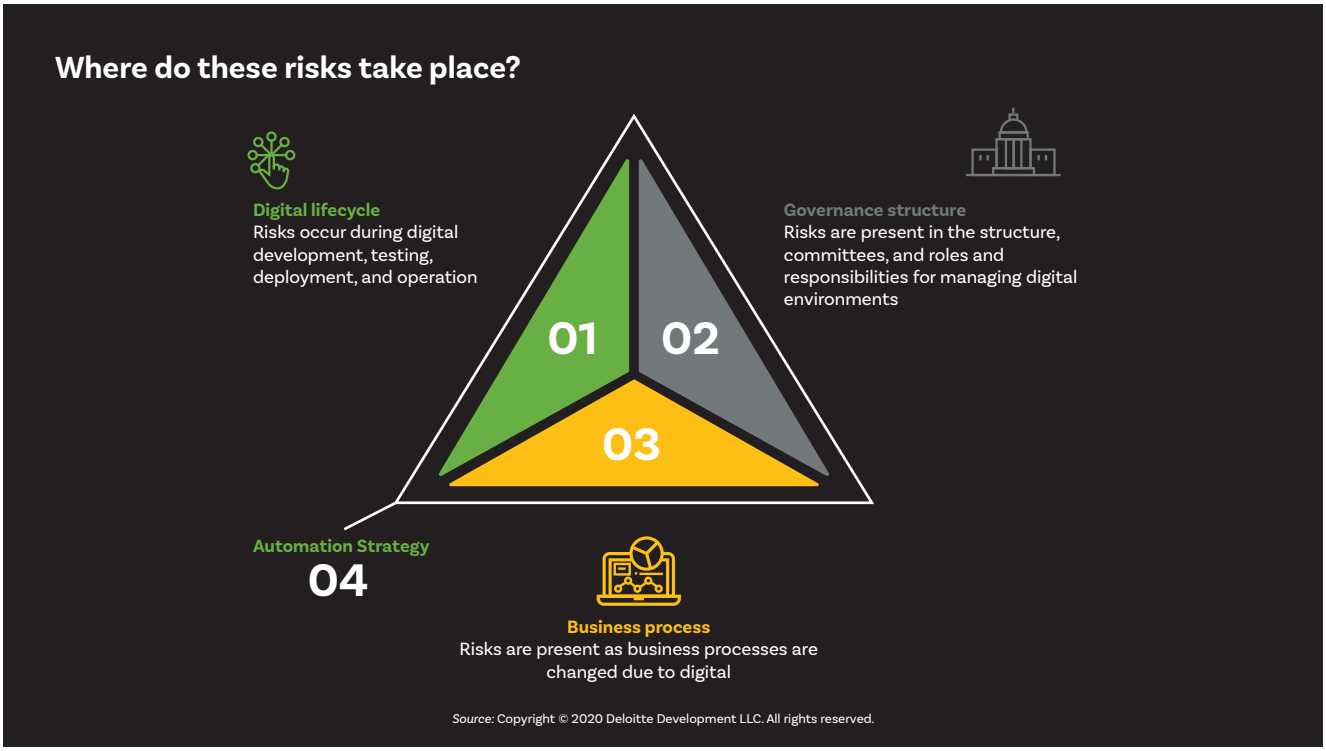
7. Artificial Intelligence (AI) Risk — Algorithm development may deliberately or inadvertently create bias, and algorithms may be used beyond intended parameters or could be impacted by poorly controlled feedback. In some cases, algorithms may suddenly shift to produce different outputs, seemingly from nowhere. A means of verifying algorithm accuracy may not even be known.

Figure 1: Seven Categories of Risks Associated with Automation



The latter category—AI Risk—is new, and it can be troubling. Companies are faced with a myriad of new considerations when leveraging cognitive technologies such as AI or machine learning. Simply demonstrating that a machine learning model is accurately doing its job can be challenging given the lack of visibility into model operations and the fluid nature of model outputs. Other considerations such as AI ethics, growing scrutiny from regulatory bodies, and the need for new development lifecycle models and governance structures must also be taken into account. In addition, instances of algorithmic bias have been known to occur, ranging from recruiting tools that were inadvertently discriminatory to chatbots that mistakenly learned to say inappropriate things. The unwanted bias in such instances can stem from flaws across three functional areas in automation: the governance model, the automation lifecycle, or within the business processes themselves. The other types of risks related to automation and cognitive technologies often take place in these three critical areas as well. To leave no stone unturned, auditors should search and test for risks across all three areas whenever and wherever automation and cognitive technologies are involved. See **figure 2**.

Figure 2: Where Automation Risk Occurs



How Can Automation and Cognitive Technologies Be Audited?

Auditing automation technologies is fast becoming a critical ability for IA teams. There are many facets of the automation audit that align closely with a traditional audit. However, auditing automation differs from auditing a manually executed process in a couple of ways. First, even though automation enables greater process standardization and execution predictability, and therefore enhances auditability of the automated process, it simultaneously introduces new risks that must be considered. Second, auditing the output of the process is no longer the main focus. Auditing automation involves a multitude of considerations beyond sampling. While it's still important to confirm that the automated process is executing properly, it is equally important to consider the new types of risks that often occur within the governance structure, the automation lifecycle, and the process controls.

Given the rapid deployment of automation tools, changing the control design post automation is one of the most commonly ignored areas of risk management. Automating a business process can alter the process control requirements. This makes it critical for IA to examine these requirements in order to gain comfort with the output from the automated process.

Overall, there are multiple aspects of process automation that elevate risk exposure as compared to a typical IT application. To determine where the greatest risks are, auditors should focus their efforts on the following critical components of the automation in addition to examining the output of the automated process:

- **Governance & Oversight** — The organizational structure for managing automation environments, including roles and responsibilities, executive sponsorship, and guidance and support from senior leadership.
  - Is there an automation operating model, such as an Automation PMO, Automation Center of Excellence (CoE), or other organizational body responsible for advocating and driving automation throughout the organization?
  - Is there alignment between the automation operating model of the CoE, technologies and vendors employed, and dev ops to reduce operational and cyber risks?
  - Is available funding aligned with the scope of the automation program? Is the funding model built to encourage and scale automation activities?
  - Does the automation program track performance and key performance indicators for each deployment as well as for the program as a whole?
  - For AI, has the right cadence of oversight meetings been established to monitor algorithm accuracy and results?

- **Planning & Alignment** — Methodologies and processes to effectively identify, value, and prioritize automation opportunities.
  - Is there a systematic methodology in place for the intake, valuation, and prioritization of automation opportunities?
  - Has the impact of the automation program on the end-to-end business process been evaluated?
  - Have automation failure scenarios been identified and contingencies planned?

- Have the appropriate people, processes, and technologies been aligned to support the scope of the automation program?
- Will the automation technology scale sufficiently to provide adequate ROI for the organization?

- **ROI** — Methodologies and processes for defining the overall cost and consequent business value of the automation program.
  - Is there a methodology in place to measure program value inclusive of qualitative benefits?
  - Has the ROI of the automation program been analyzed to determine whether it will provide sufficient value? Have post-release lessons learned been considered?
  - Is the selected automation technology or vendor providing the best value to the organization in the long term?
  - Has the potential for and impact of automation failure been adequately factored into the ROI calculation?

- **Policies & Procedures** — Protocols for managing risks associated with automation technologies.
  - Are policies and procedures being revised to address the automation program?
  - Does the business consider the risk and compliance obligations of its automation programs?
  - Are there policies and procedures in place for areas such as business continuity, regulatory compliance, data leakage and privacy, cyber threats, incident management, identity and access management, change management, and exception handling?

- **Development Standards** — Expectations for the development, testing, and deployment of automation technologies.
  - Is there a robust development, testing, and deployment methodology for automation solutions?
  - Have automation development standards been defined?
  - Are there controls implemented to address automation development, testing, and deployment?
  - Have an adequate number of different and unusual test scenarios been defined?
  - Does the business test, accept, and sign off on automations?

- **Controls** — Processes to manage the first and second lines of defense (e.g., operations and risk management, and risk oversight, respectively.)
  - Have controls been implemented in alignment with the expected process requirements?
  - Is the impact of the automation program on the control environment being evaluated?
  - Has the organizational risk and control framework been modified to align with the automation program?
  - Will these risks and controls be evaluated on an ongoing basis by the IA department?

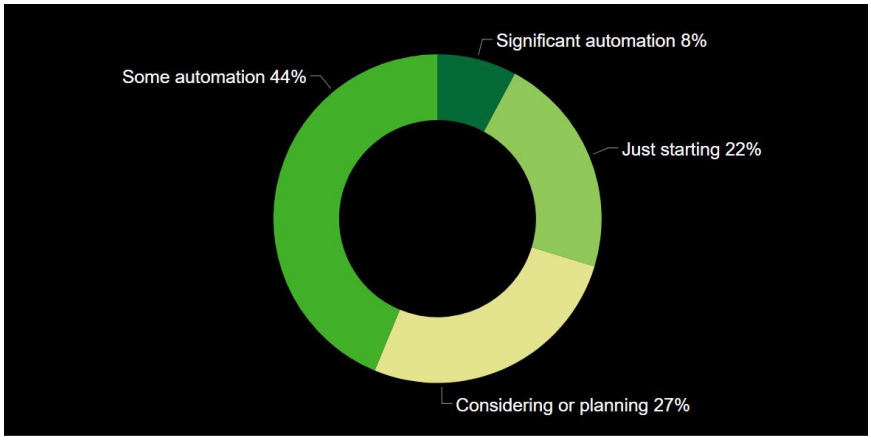
Naturally, in order for IA to be able to consider all of the critical components of the automation lifecycle, there will be an investment required in order to up-skill and educate existing auditors on the leading practices and standards of the automation technologies. As capabilities of IA teams mature, so should their ability to provide greater assurance to the business that their investment in automation not only can provide financial return, but also that the new risks associated with these technologies have been considered and accounted for.

Digital Survey Findings

To provide insight into where different IA organizations stand with respect to auditing automation and cognitive technologies, Deloitte recently conducted an online survey among IIA members. Based on 64 responses from IA leaders across a broad range of companies, the following key findings shed light upon where many IA organizations are making progress and where gaps may still remain:

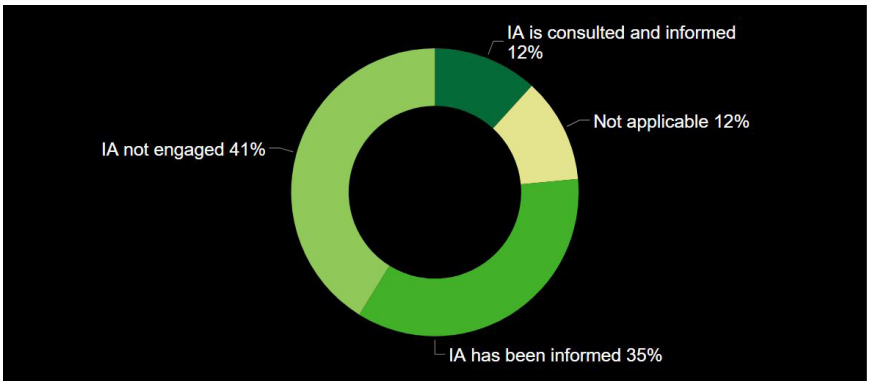
Of the organizations surveyed, 27% are considering or planning automation capabilities, while 22% are just starting with a proof of concept.

How mature is the automation capability within your organization?



Of respondents in the planning stage, 35% reported that IA has been informed of the intentions to automate and it has a seat at the table in providing its perspective on risks. A total of 12% said that IA is both consulted and informed with regard to intended automations, with a review of automation capabilities being planned. For the 53% of responding companies in the planning stage where IA is not engaged, now is the time to act. There is a significant opportunity for IA to become more involved from a risk perspective in automation planning.

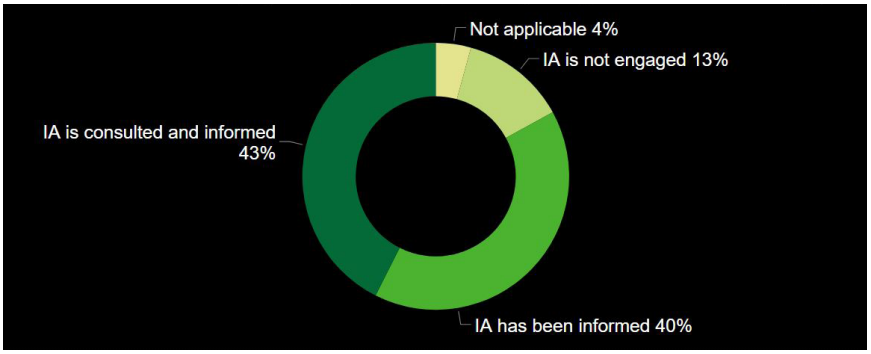
For organizations *considering or planning for automation capabilities*: What role has internal audit played during the development of your organization's automation program?



Of surveyed organizations, 73% have at least some automation capabilities. These organizations are at various stages of development. A total of 22% of respondents are just starting with automation, while 44% have some automation in place. Only 8% reported having significant automation activities. This suggests that automation technologies are progressing in terms of adoption, but they are far from maturity.

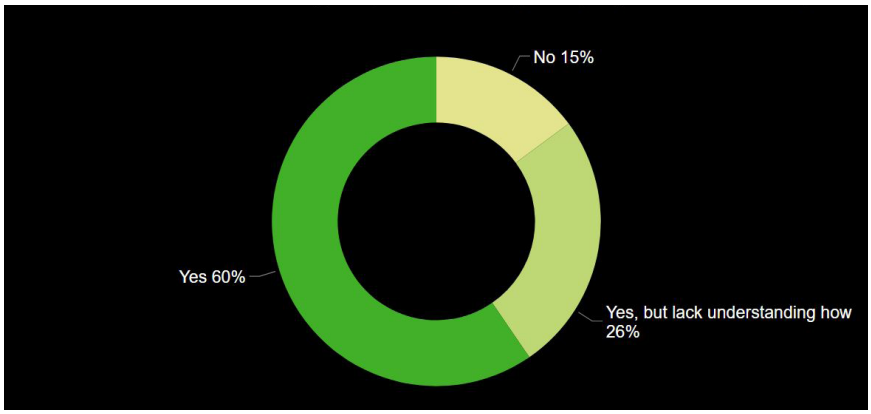
For those responding organizations that have some level of automation capability in place, 13% said that IA is not engaged; 40% indicated IA is informed and provides perspectives to the business on risks; and 43% said IA is consulted and informed and is planning a review of automation capabilities. For IA organizations that are not engaged or informed (only 17% of respondents), this highlights a significant opportunity for greater IA involvement in automation capabilities.

For organizations that had *some level of automation in place* (starting, some, significant): What role has internal audit played during the development of your organization's automation program?



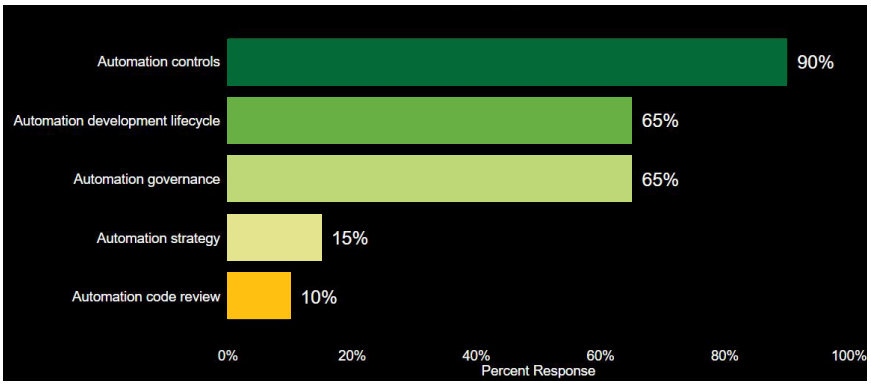
For responding organizations that have some automation capabilities, 60% of IA departments indicated they understand the technology and have included it in their work. Only 15% said they are not planning on including automation technologies in their IA work. Perhaps most intriguing, 26% of IA organizations know they should include automation technologies as part of their review, but they don't have a clear understanding of how to do so. This shows there is good awareness of the need to review these technologies, but there is still a significant opportunity for IA to learn more, including acquiring greater familiarity with automation testing frameworks and methodologies.

Where IA is consulted and informed or planning a review of automation capabilities: Is the audit of automation technology and processes part of your ongoing annual internal audit plan?



Where IA is consulted and informed, and IA has reviewed or plans to review automation capabilities, additional survey questions were asked to assess the focus of the IA review. Respondents indicated a heavy emphasis on controls review (90%); a secondary focus on governance (65%) and development lifecycle (65%); and a smaller focus on strategy (15%) and code (10%). This highlights a significant opportunity for IA to be more involved in reviewing automation strategy. Greater involvement is important to fully understanding the impact of automation upon the organization and to inform planning.

For responding organizations that had *some level of automation in place* (starting, some, significant) and where internal audit *is consulted and informed or is planning a review* of automation capabilities: Where internal audit has or plans to review the automation capabilities, what is the focus of that review?



Risk to ROI

New technology is often accompanied by ambiguity around its effectiveness and value. Because automation and cognitive technologies demand heavy lifting in terms of planning, development, configuration, and testing, the risk they pose to ROI can be significant. Automation deployment can be costly and sometimes it can be difficult to determine if the investment is going to be worthwhile. In other cases, the potential rewards may be clear, but the development and execution can go off track. For instance, company resources could be wasted on planning and developing a bot that is ineffective or that is abandoned by the business. Or, the impact of unforeseen processing errors caused through misconfiguration, unanticipated changes in data inputs, or insufficient business testing scenarios could limit the value obtained. The inability to scale also poses a significant risk to value realization. Meanwhile, failed automation attempts could cause business leaders to lose confidence in automation technologies, which can lead to unrealized efficiencies and missed opportunities. These potential shortfalls give IA an opportunity to play an advisory role, since most unsuccessful or disappointing automation attempts can be traced to risks that were not anticipated and/or managed properly.

IA can provide an additional level of assurance and objective reasoning to management about whether or not the company is spending money wisely and if it is likely to receive a sufficient return on its automation investment. Furthermore, if a business unit is implementing automation and cognitive technologies, IA should be able to ask if there is financial reasoning behind the investment, what the basis for this reasoning is, and if mechanisms are in place to track returns. It should also be able to assess whether the technology being implemented can be scaled across the enterprise, which is often a critical factor in realizing sufficient ROI.

Conclusion

The internal auditor is now working in a digital world—one that will extend traditional risk boundaries into uncharted territory. While there are common risk themes associated with automation and cognitive technologies, their transformative nature puts a unique twist on common practices, such as segregation of duties. This makes missteps potentially more severe and subsequently more harmful to ROI.

As companies embrace change through automation, IA organizations must follow suit and adapt their approach to the expanding digital landscape. As reflected in the survey findings, despite growing involvement by IA, there is still a significant opportunity to go deeper and to add more value. Now is the time for IA to embark on the automation journey alongside the business, if it hasn't already done so, and for IA teams to enhance their understanding of how they can contribute to safer and more rewarding business outcomes.

In a digital world, auditing the processing output is no longer the main focus. Assurance over the integrity of the end-to-end business process after automation has been introduced, and control over the automation program as a whole, are the overarching goals. Accordingly, effective automation audits do not occur exclusively at the level of traditional control tests, though some of these tests will still be required. Necessary evidence to evaluate risk should also be obtained through interviews and high-level fieldwork.

Ultimately, the success of an enterprise automation program will likely come down to its ability to scale with efficiency and effectiveness. The program must provide value, while the business must commensurately address the risks threatening that value. Here, IA can play a valuable advisory role by providing insight into leading practices for reducing risk as well as being a guiding light for increasing ROI.

Deep-Dive Examples of Automation Risk

- **Account management and segregation of duties (SoD) in the bot development lifecycle:** While most companies have strong account management and SoD procedures in place for regular system development, bot development often falls below the radar. During the first year of implementing automation, a company may have only a few people, or even a single person, managing bot development and maintaining automation software. This can increase risk in many respects. First, the typical procedural and access restrictions to development, testing, and implementation may not exist, and one person may have access to everything. Second, the bots themselves often need to access sensitive internal systems. Since bots interact with systems as a human would, by populating the user name and password fields, they must have access to production passwords. While SoD would commonly come into play if humans were doing this work, bots are often not barred from accessing multiple systems, which together could allow for fraud or other misuse. And, bots evoke yet another SoD concern. While the system passwords accessed by bots are commonly encrypted, a developer does not need to know the password, only how to develop a bot to use it. Thus, in many environments, it is conceivable that an automation developer could build and launch a bot that is able to bypass normal SoD controls.

  SoD as it relates to bots raises several thought-provoking questions that require careful analysis. Should bots follow the SoD principles as a human employee would, or should they be trusted more because they are not human? Should dozens of bots be coded separately with appropriate handoffs that enforce segregation, or should one end-to-end bot be created, even though it could potentially have toxic combinations of access? Should the bots be limited in a way that a developer can code or that operations personnel can access so as not to violate SoD principles? The answers to these questions have potential implications for not only operational efficiency, but also security.

- **Operational risk stemming from confusion around ownership of automation:** While automation software has become commonplace in many companies, there is still a lot of confusion around who should own and manage not only the technology but also the strategy around its use. It is common for IT to have a central role, which often expands beyond the management of the technology to the strategy behind its use. Automation and cognitive technologies are less like a tool that does a task and more like a new type of employee. Without a cross-functional team with representation from the business unit impacted, IT, IA, and even human resources, automation technology is often applied in a way that significantly limits its potential to drive strategic change. This lack of visible impact often leads to questions about the worth of the software and further curtails executive sponsorship of future programs. In addition, there is often confusion around the business unit's role in managing this new type of "worker," which can lead to insufficient involvement and poor oversight of a bot's performance.

- **AI risk:** AI technologies, especially predictive models, are widely used throughout many industries, ranging from consumer products to financial services. However, it is the intersection of AI with socially sensitive areas such as criminal justice and health care that causes many to take pause. For example, machine learning is making its way into health care as an industry-wide method of predicting risk. For instance, hospitals, health systems, insurance companies, and government agencies are increasingly turning to AI to predict which patients may benefit most from care-management programs and to target them accordingly. This type of bias can potentially emerge from the design of the algorithm, from the outcome the algorithm is asked to predict, or from inequities in the underlying data. This illustrates the complexity of being fair and remaining compliant when developing and implementing AI technologies. Traditional development approaches often do not have the agility required by AI, and normal testing approaches often fail as predictive models do not have a single expected result.

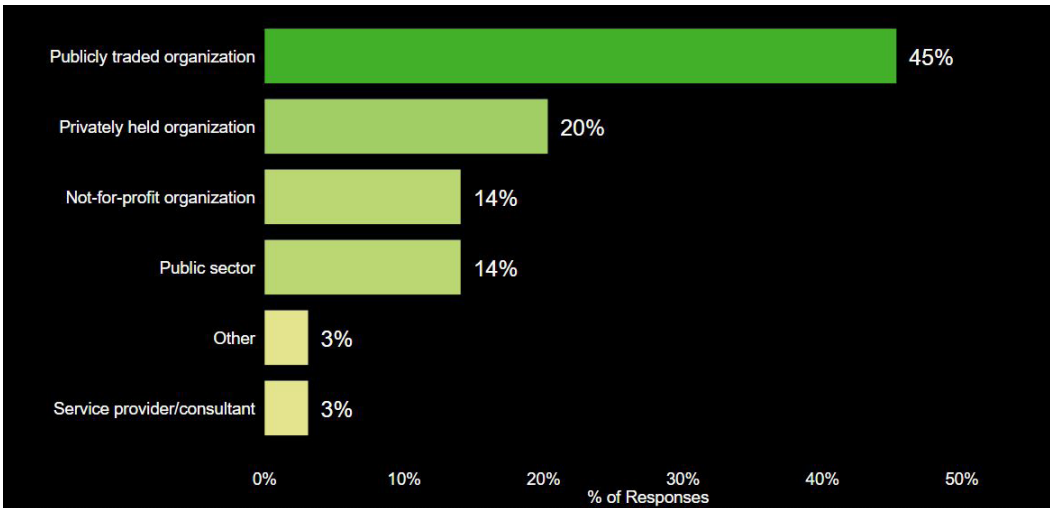
[2] Ziad Obermeyer, Brian Powers, Christine Vogeli, and Sendhil Mullainathan, "Algorithmic bias in health care: a path forward," *Health Affairs*, November 1, 2019, https://www.healthaffairs.org/do/10.1377/hblog20191031.373615/full/.

Appendix

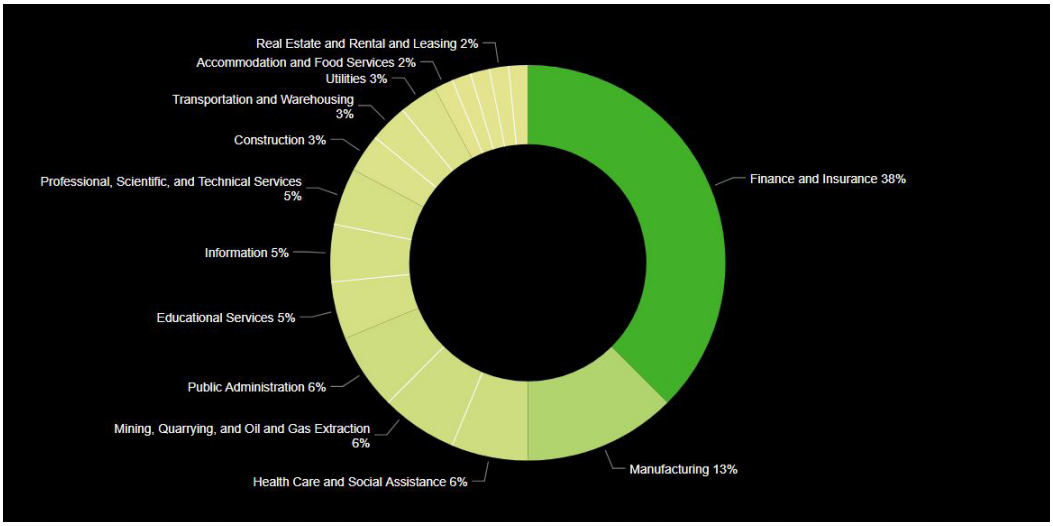
Survey Results

Below are the results of the referenced survey to IIA members. There were 64 respondents from a variety of countries, industries, and organizational structures (public, private, and nonprofit). Some of the questions were conditional (i.e., questions were presented based on a specific previous response). The graphs display percentages, which are either percentages of the 64 respondents or the subset of the 64 that received the conditional question.

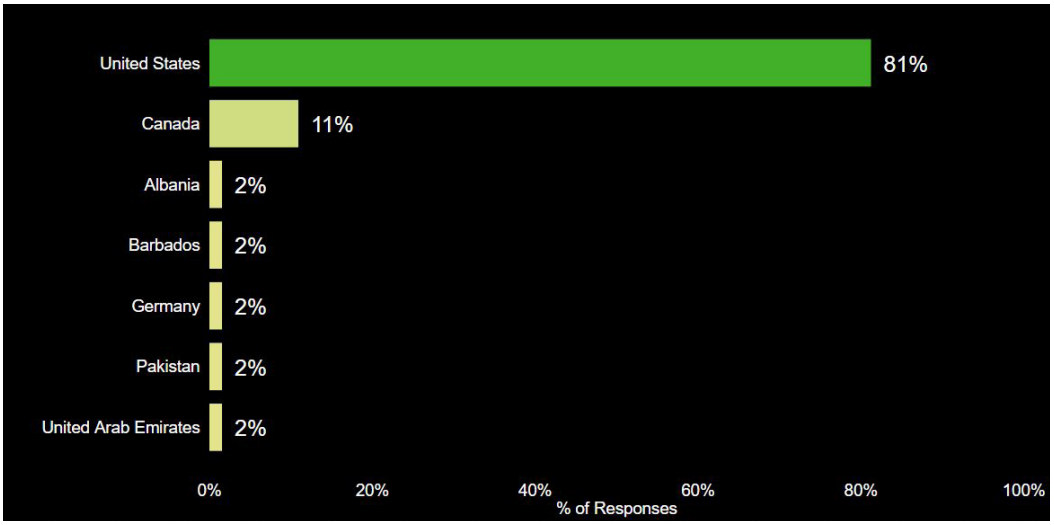
For which type of organization do you currently work?



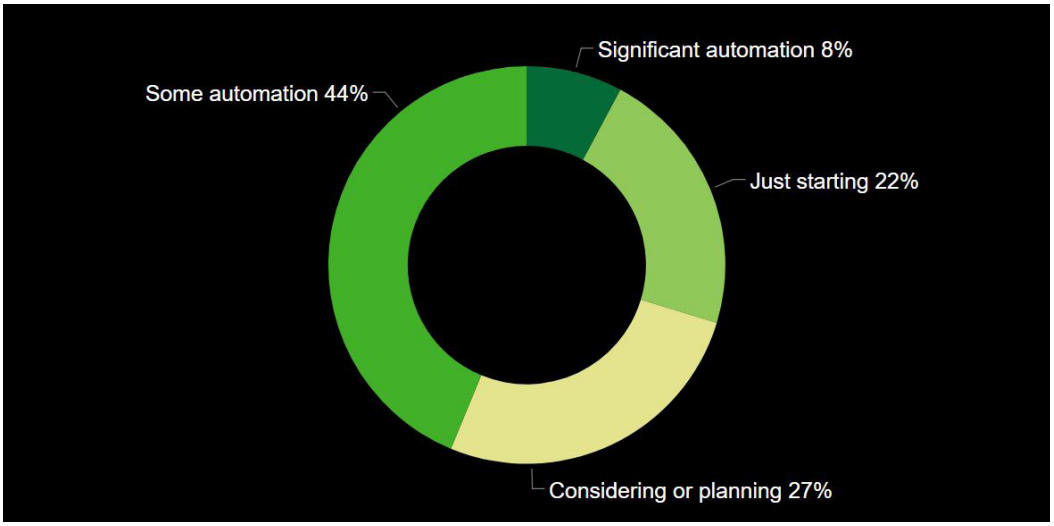
Primary industry distribution:



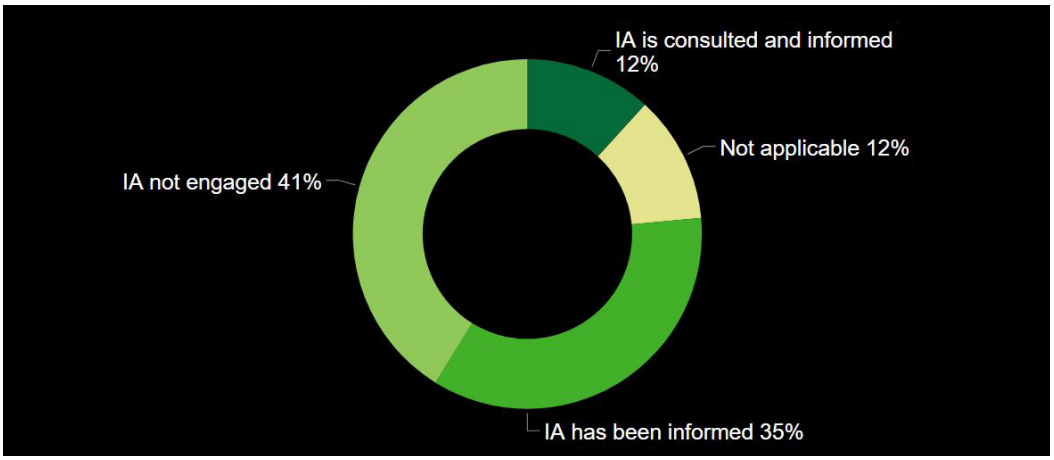
Responder's country:



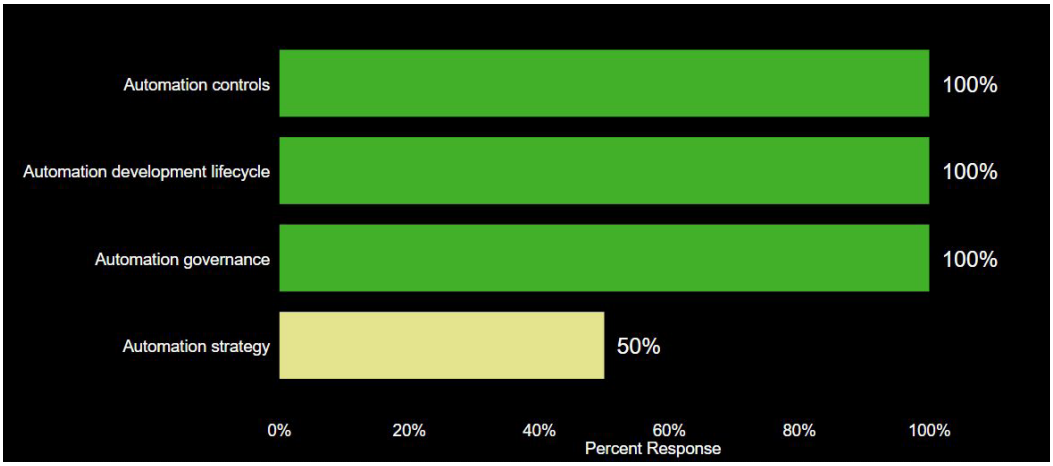
How mature is the automation capability within your organization?



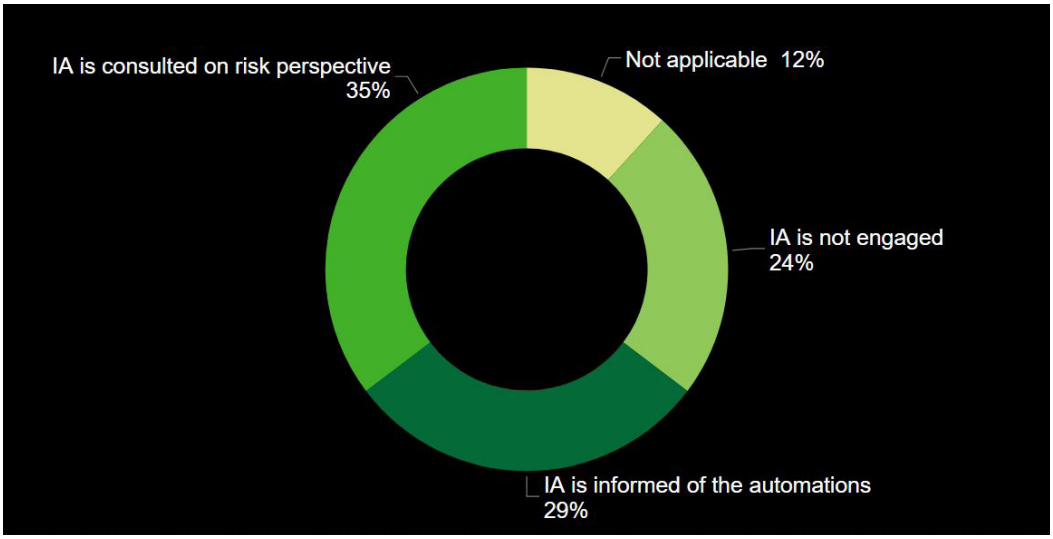
For organizations *considering or planning for automation capabilities:* What role has IA played during the development of your organization's automation program?



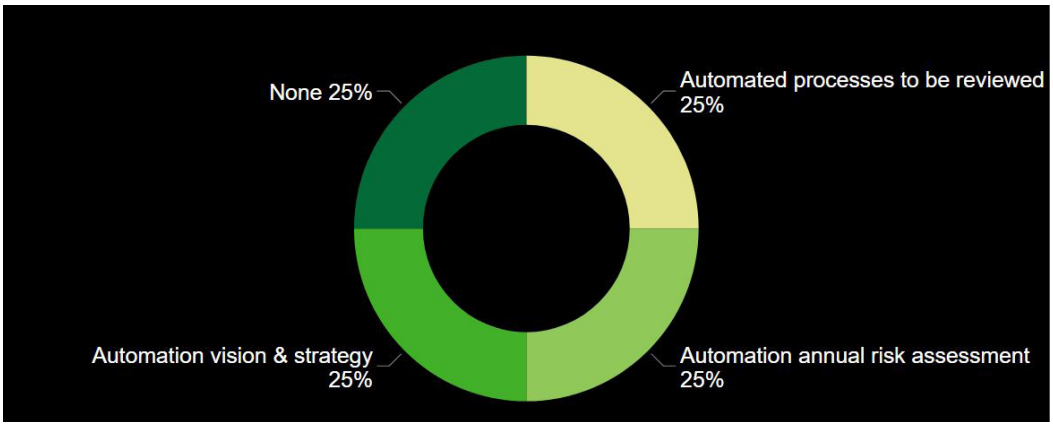
For *organizations considering or planning for automation capabilities and where internal audit is consulted and informed or is planning a review* of automation capabilities: Where IA has or plans to review the automation capabilities, the focus of that review is:



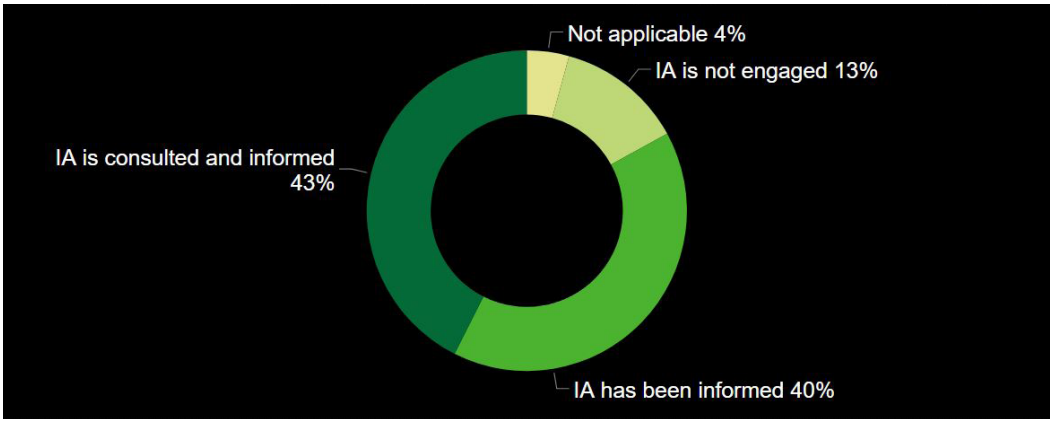
What role does internal audit have during the implementation of the new automation technology?



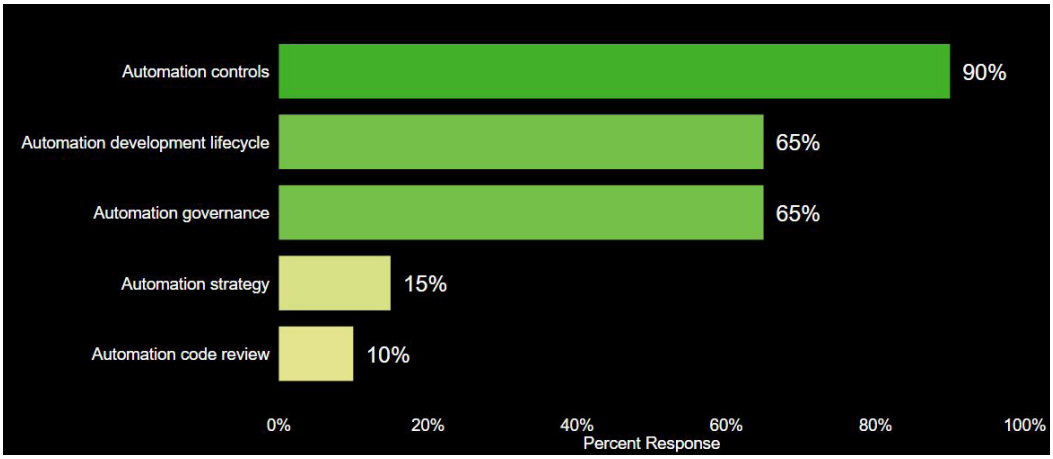
What role do you expect internal audit to have in the future?



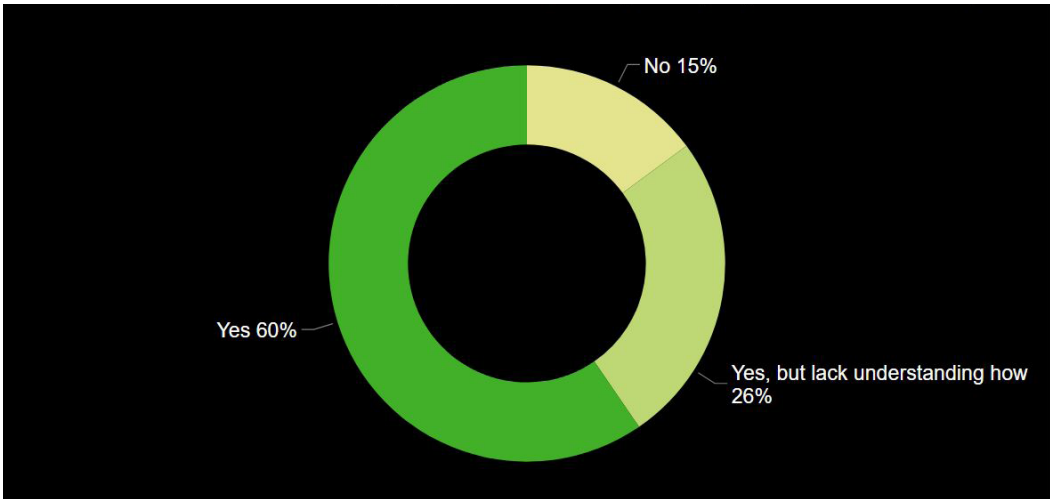
For organizations that had *some level of automation in place* (starting, some, significant): What role has internal audit played during the development of your organization's automation program?



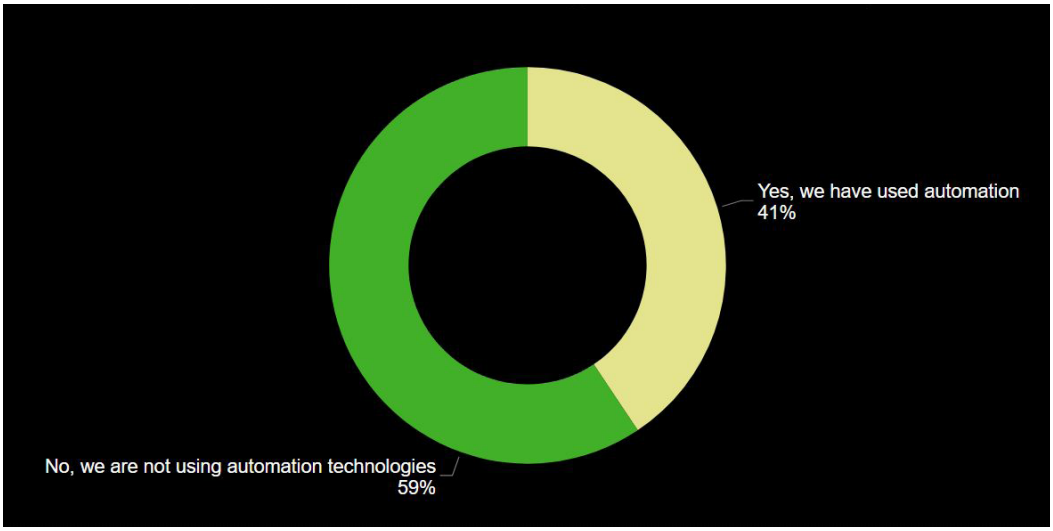
For responding organizations that had *some level of automation in place* (starting, some, significant) and where internal audit *is consulted and informed or is planning a review* of automation capabilities: Where internal audit has or plans to review the automation capabilities, what is the focus of that review?



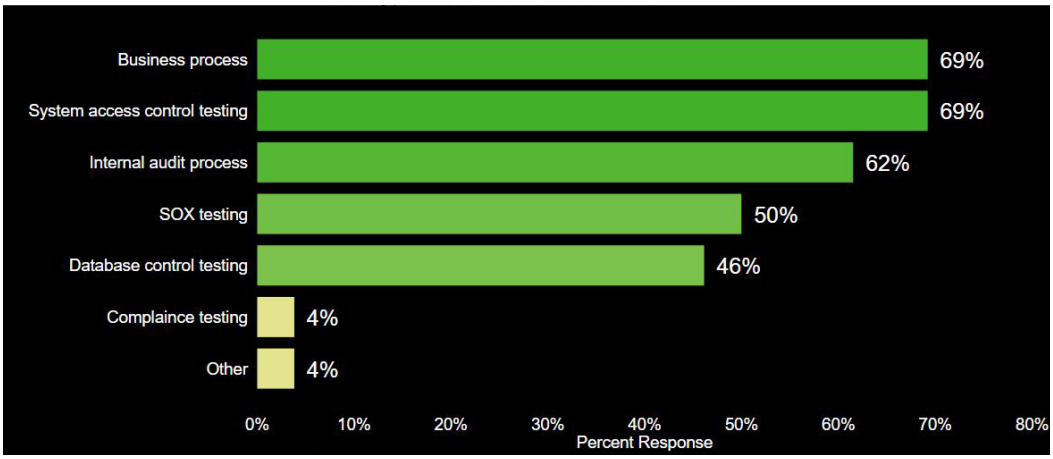
Where IA is consulted & informed or planning a review of automation capabilities: Is the audit of automation technology and processes part of your ongoing annual internal audit plan?



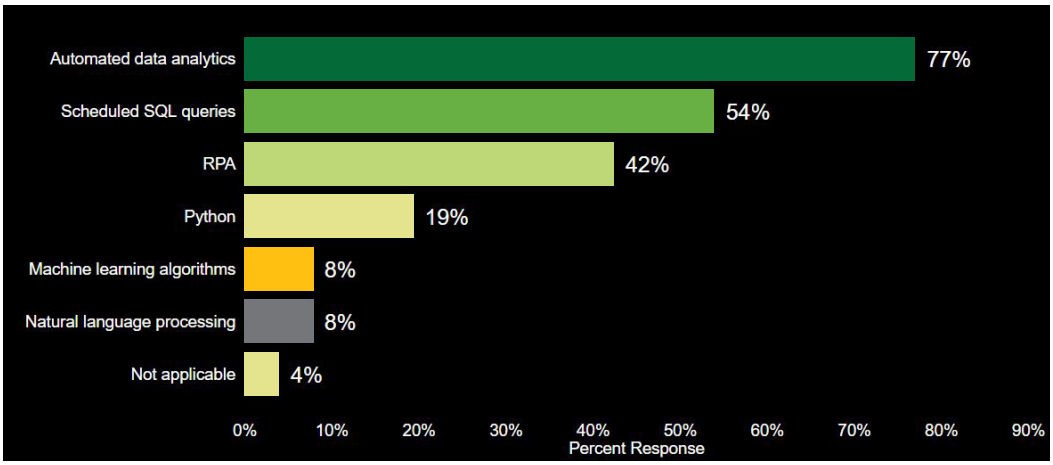
Is the audit planning or using automation technology within the internal audit scope of work?



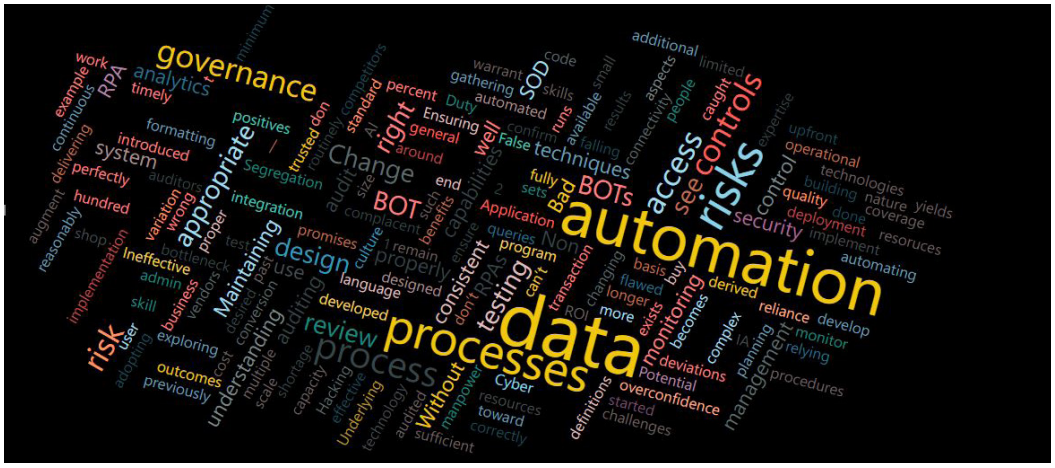
What type of audits have used automation?



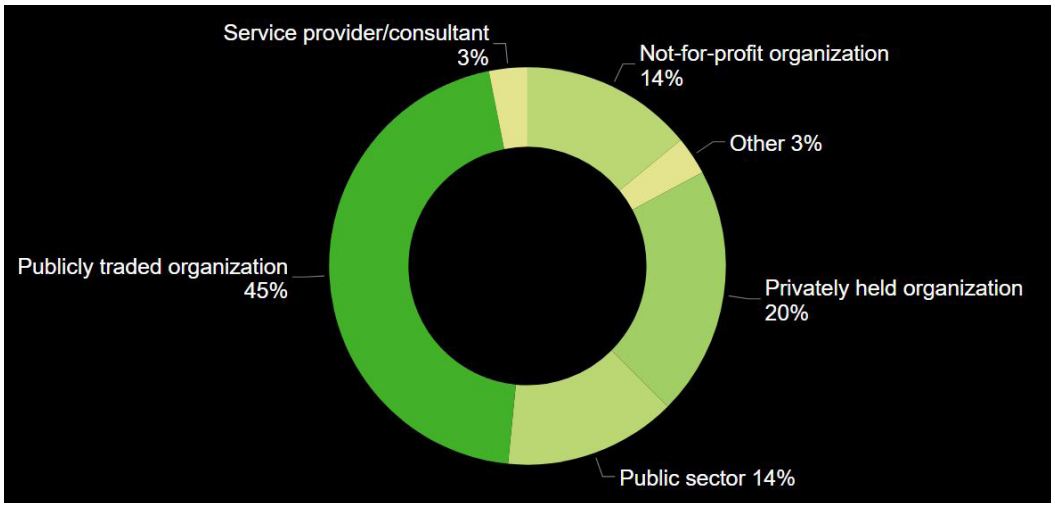
What automation technologies are you leveraging within internal audit?



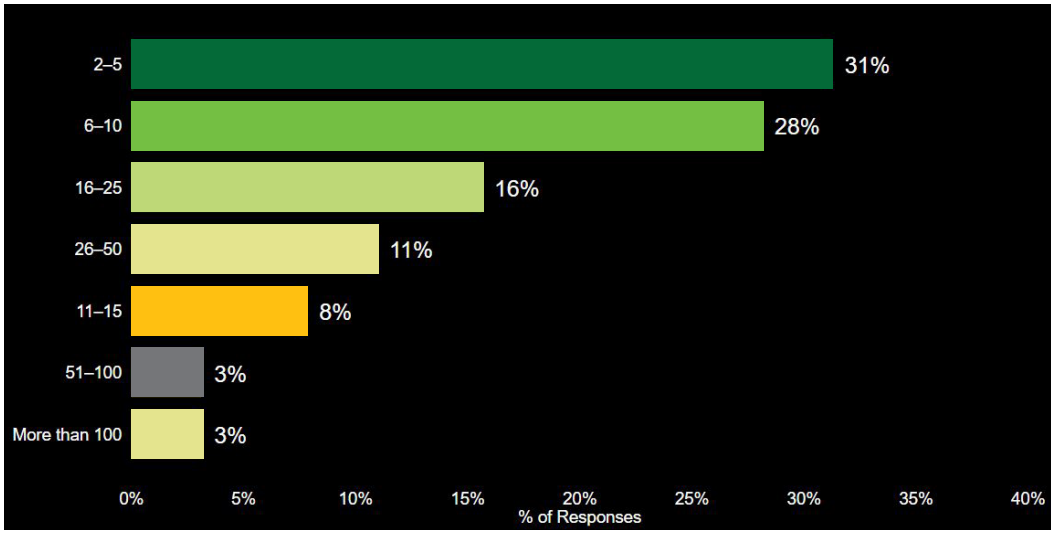
What are the risks that you see from introducing the automation technology to your organization? Repetition factor = 1



For which type of organization do you currently work?



What is the size of your internal audit function?



Contacts

Neil White
Principal
Deloitte & Touche LLP
nwhite@deloitte.com

Michael Schor
Partner
Deloitte & Touche LLP
mschor@deloitte.com

Martin Rogulja
Senior Manager
Deloitte & Touche LLP
mrogulja@deloitte.com

Mike Koppelmann
Senior Manager
Deloitte & Touche LLP
mkoppelmann@deloitte.com

Contributors

Patrick Girling
Manager
Deloitte & Touche LLP
pgirling@deloitte.com

Asef Qayyum
Consultant
Deloitte & Touche LLP
aqayyum@deloitte.com

2020-0246