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

Automation Risk Framework – the Mandate for Good Governance 4
How Can Automation and Cognitive Technologies Be Audited? 7
- **Governance & Oversight** 8
- **Planning & Alignment** 8
- **ROI** 9
- **Policies & Procedures** 9
- **Development Standards** 9
- **Controls** 10

Digital Survey Findings 11
Risk to ROI 14
Conclusion 15
Deep-Dive Examples of Automation Risk 16
Appendix: Survey Results 17

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.

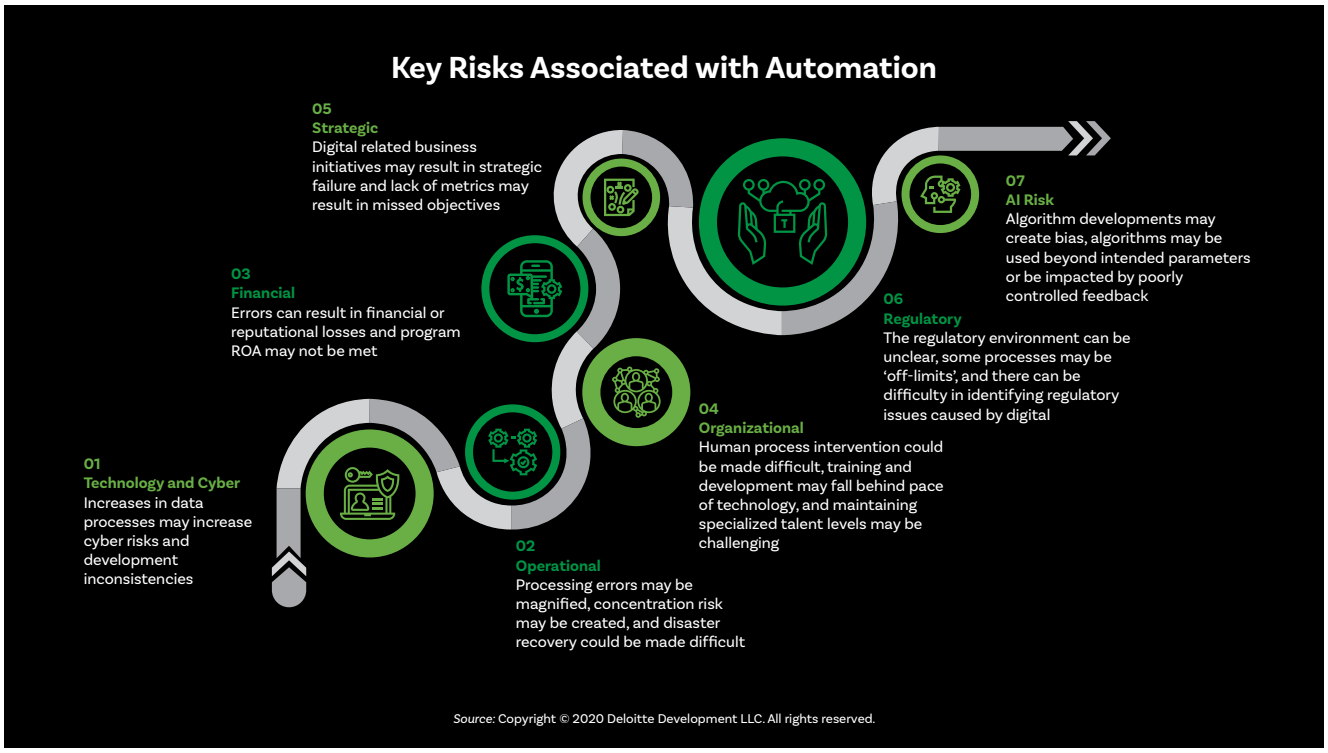
4. Strategic Risk — Automation-related business initiatives may lead to strategic failure and lack of metrics may result in missed objectives.

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.

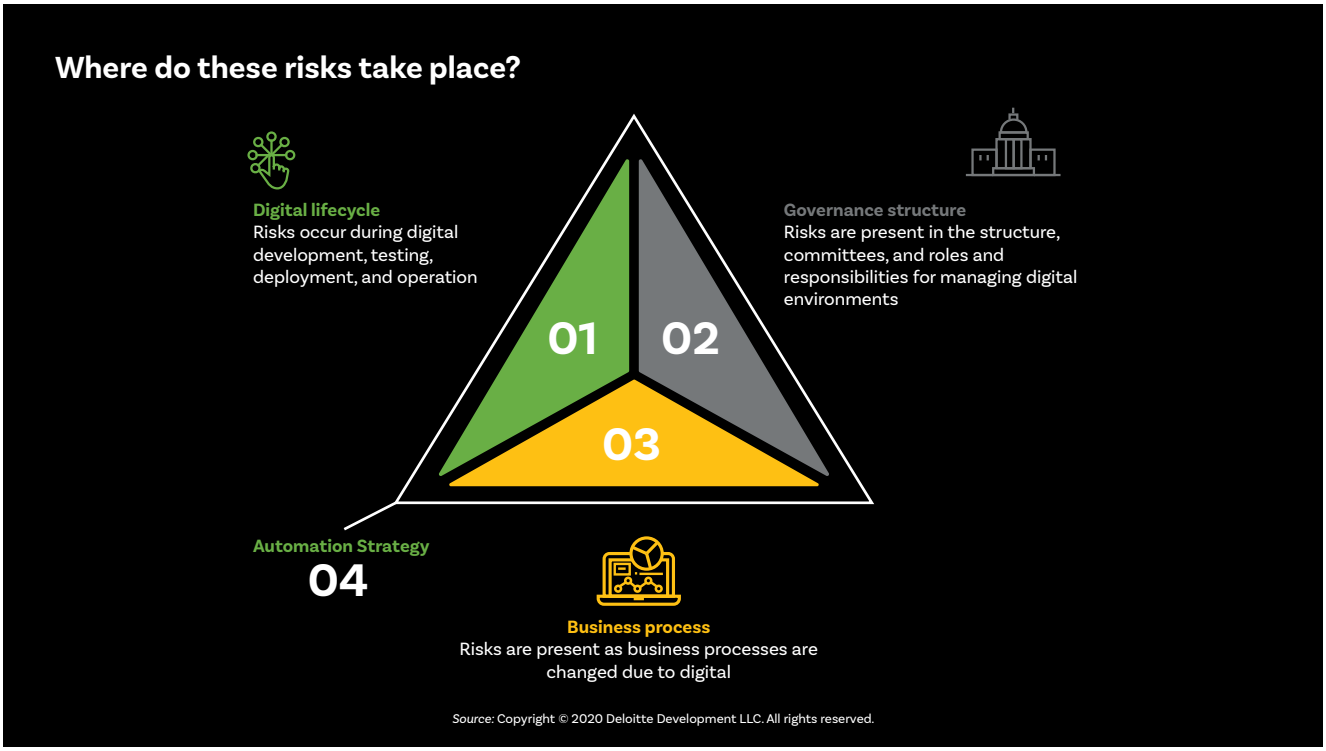
7. Artificial Intelligence (AI) Risk — Algorithm development may deliberately or inadvertently create bias, and algorithms may be used beyond intended parameters or could be impacted by poorly controlled feedback. In some cases, algorithms may suddenly shift to produce different outputs, seemingly from 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?

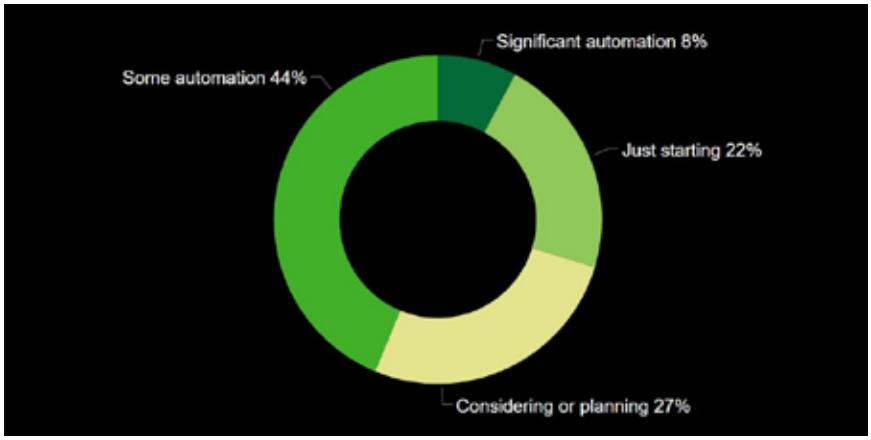
Naturally, in order for IA to be able to consider all of the critical components of the automation lifecycle, there will be an investment required in order to up-skill and educate existing auditors on the leading practices and standards of the automation technologies. As capabilities of IA teams mature, 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:

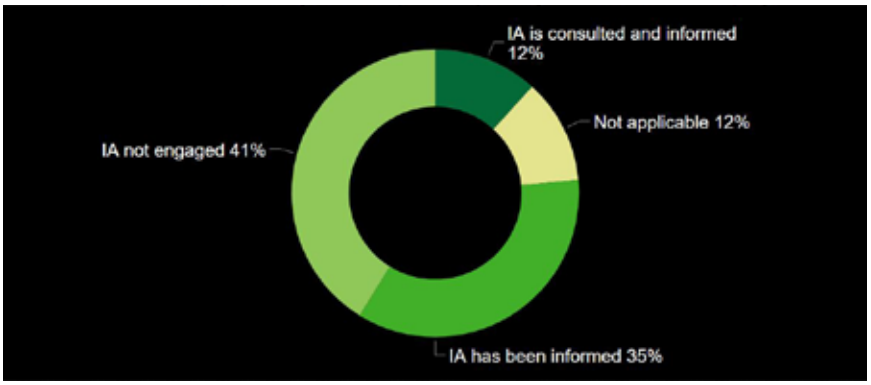
Of the organizations surveyed, 27% are considering or planning automation capabilities, while 22% are just starting with a proof of concept.

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.

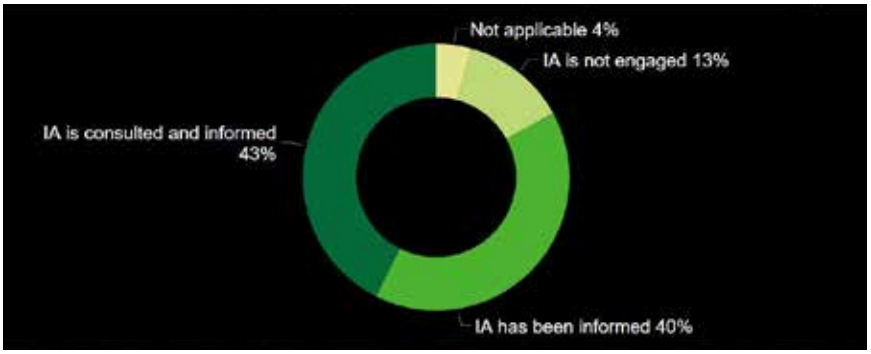
For organizations *considering or planning for automation capabilities*: What role has internal audit played during the development of your organization's automation program?



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.

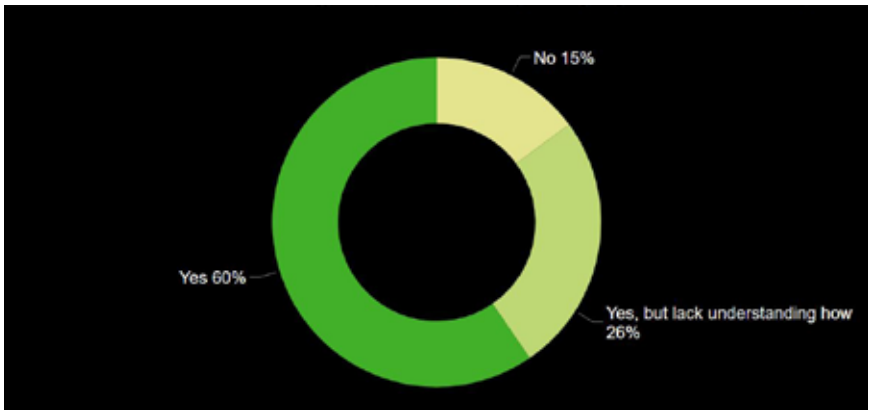
For those responding organizations that have some level of automation capability in place, 13% said that IA is not engaged; 40% indicated IA is informed and provides perspectives to the business on risks; and 43% said IA is consulted and informed and is planning a review of automation capabilities. For 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?



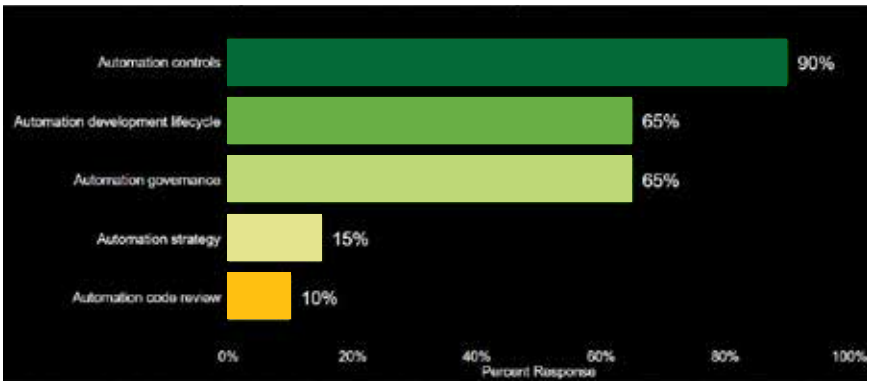
For responding organizations that have some automation capabilities, 60% of IA departments indicated they understand the technology and have included it in their work. Only 15% said they are not planning on including automation technologies in their IA work. Perhaps most intriguing, 26% of IA organizations 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.

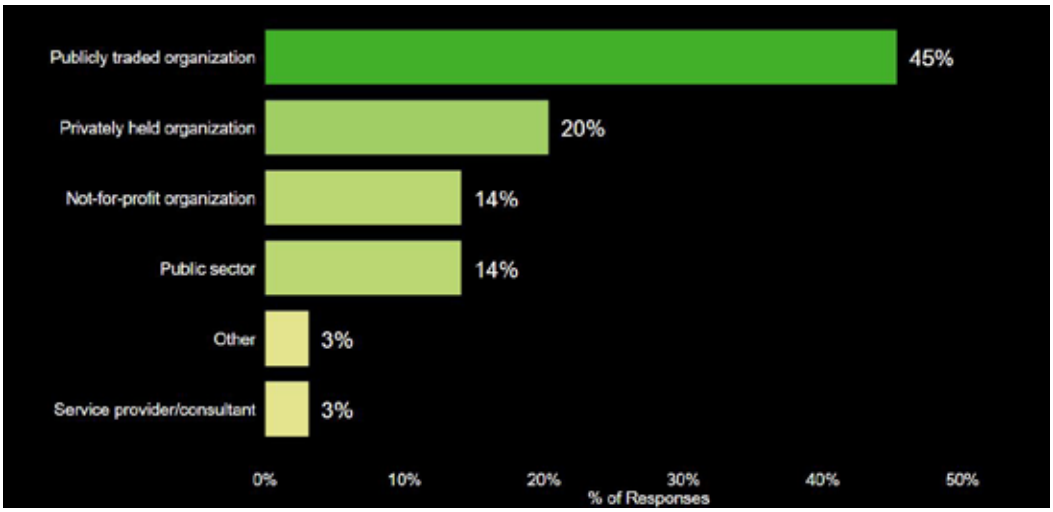
[2] Ziad Obermeyer, Brian Powers, Christine Vogeli, and Sendhil Mullainathan, "Algorithmic bias in health care: a path forward," *Health Affairs*, November 1, 2019, https://www.healthaffairs.org/do/10.1377/hblog20191031.373615/full/.

Appendix

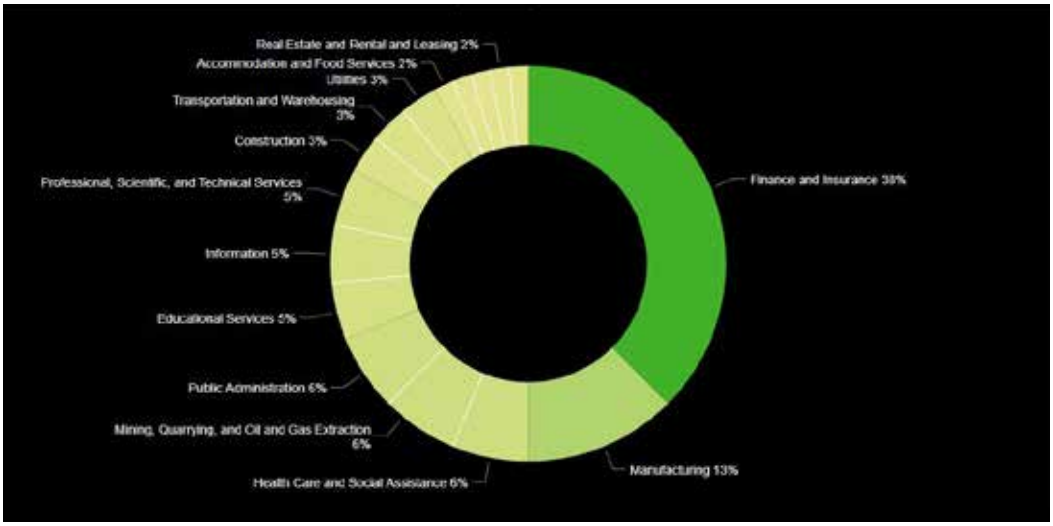
Survey Results

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.

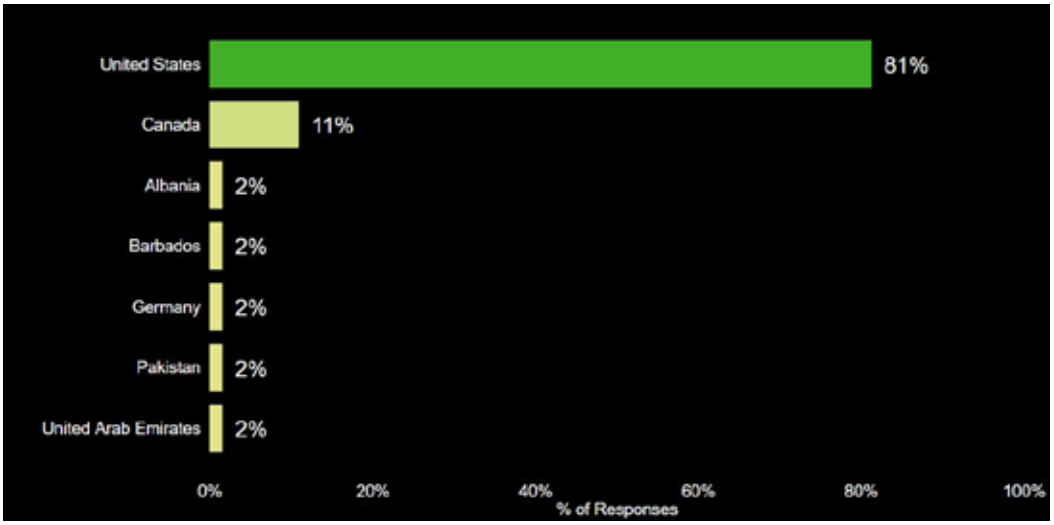
For which type of organization do you currently work?



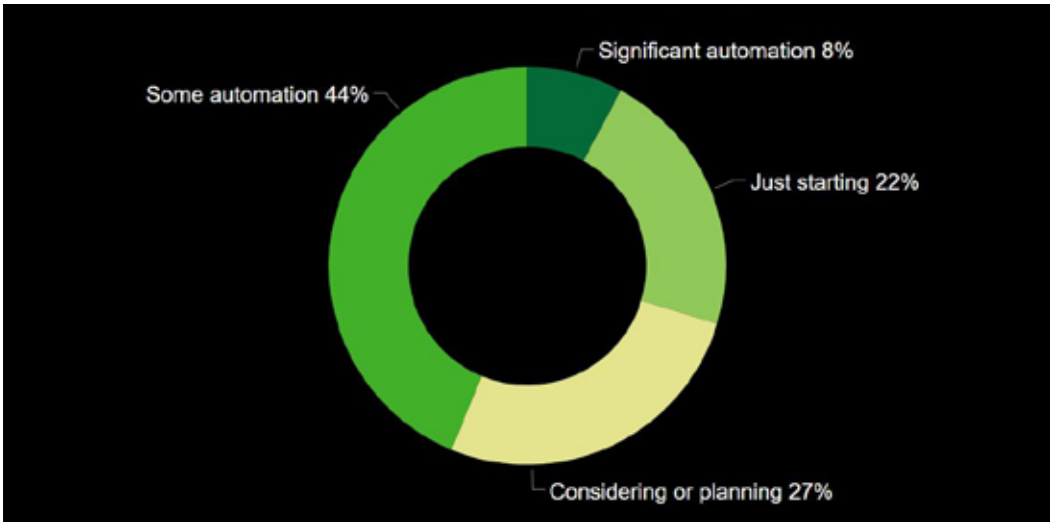
Primary industry distribution:



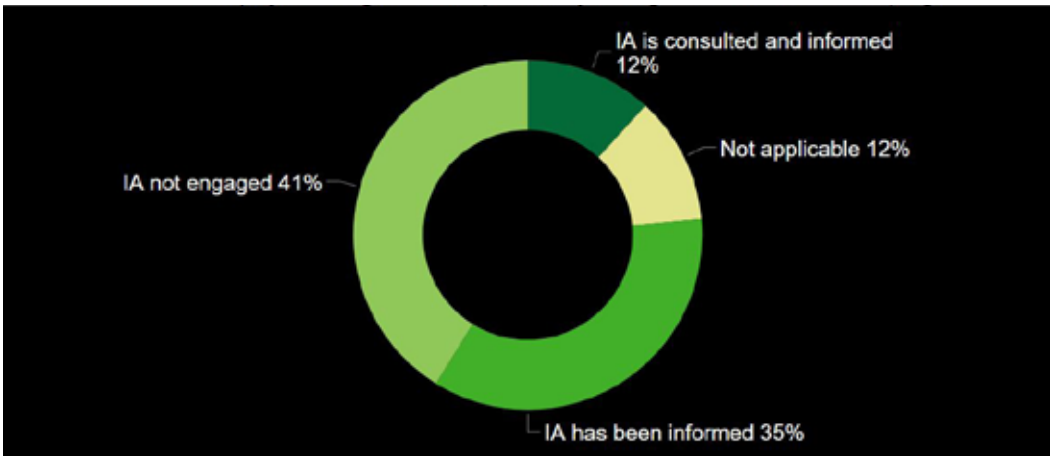
Responder's country:



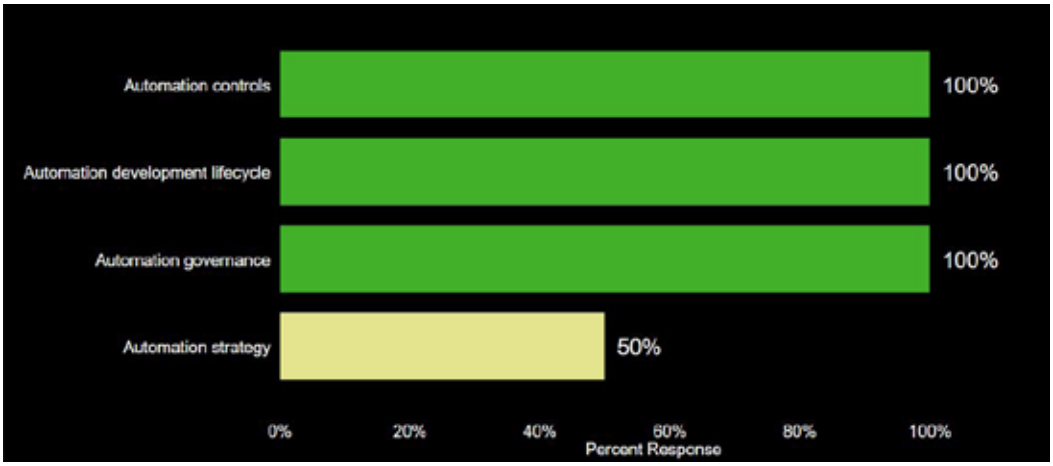
How mature is the automation capability within your organization?



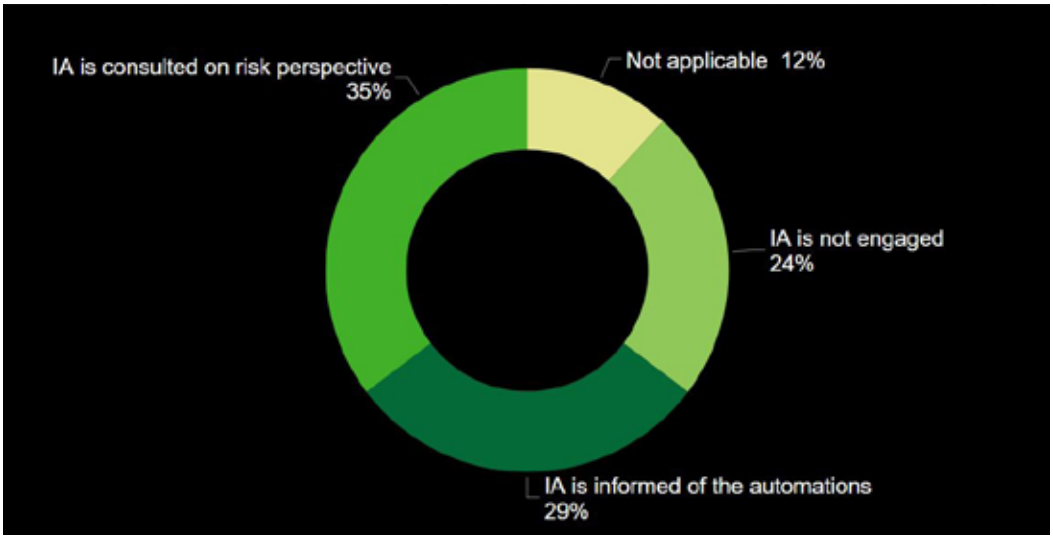
For organizations *considering or planning for automation capabilities:* What role has IA played during the development of your organization's automation program?



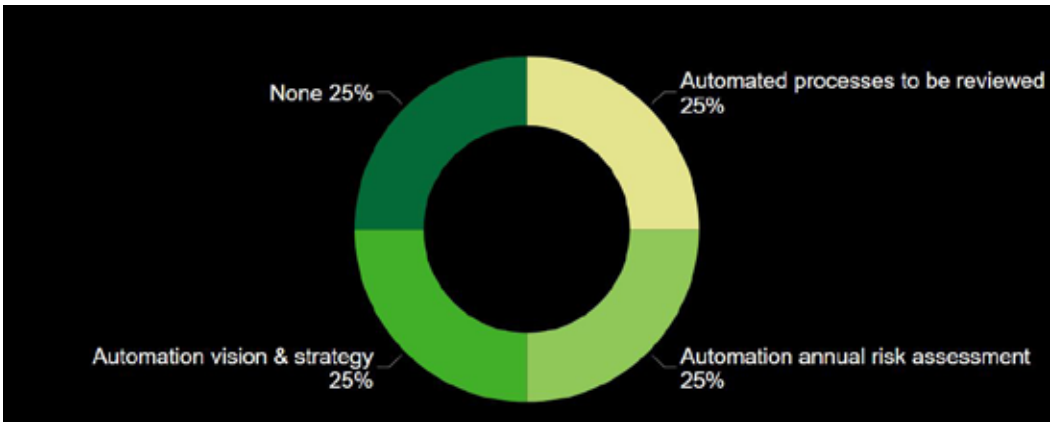
For *organizations considering or planning for automation capabilities and where internal audit is consulted and informed or is planning a review* of automation capabilities: Where IA has or plans to review the automation capabilities, the focus of that review is:



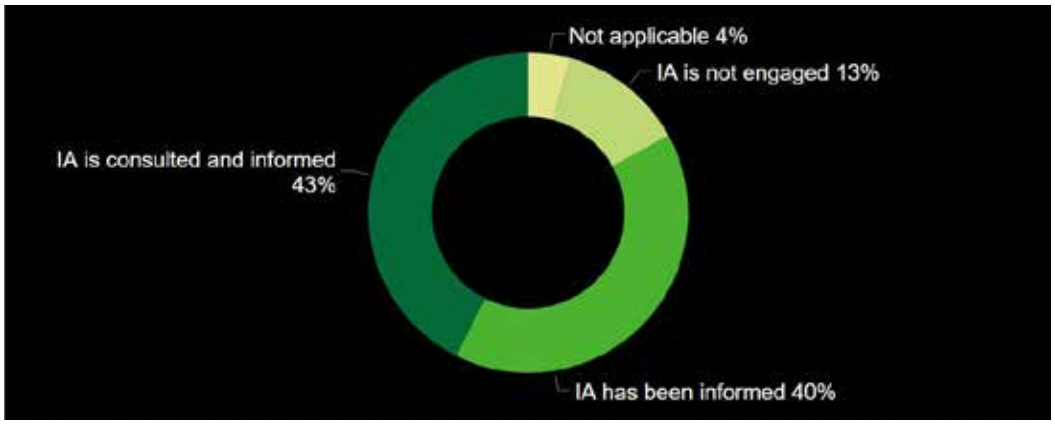
What role does internal audit have during the implementation of the new automation technology?



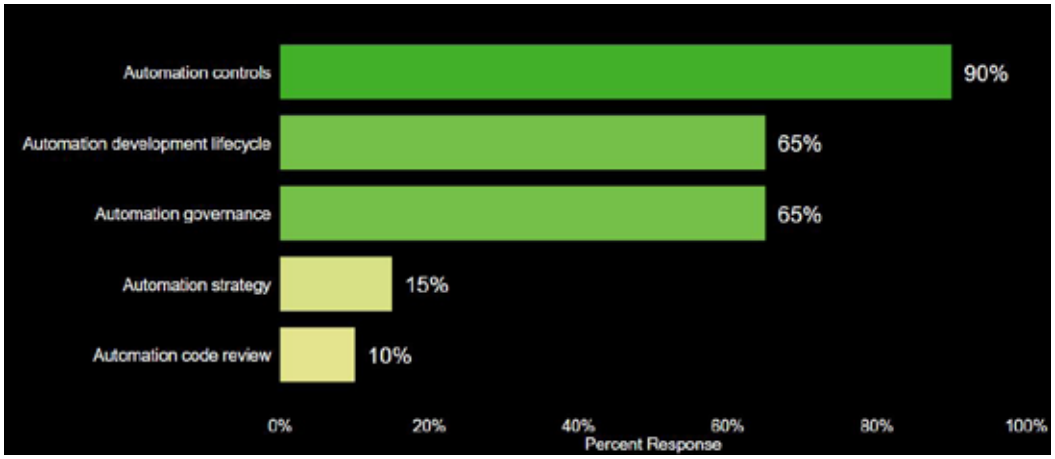
What role do you expect internal audit to have in the future?



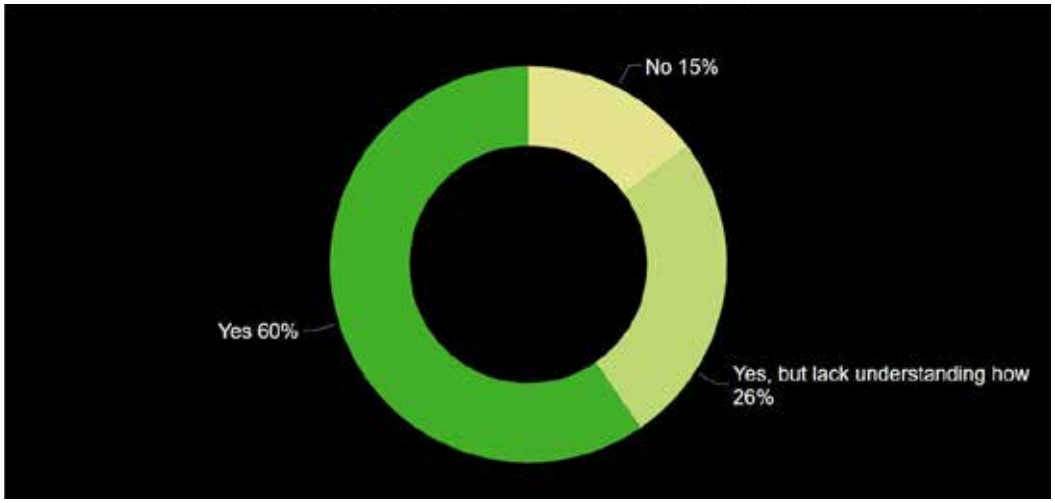
For organizations that had *some level of automation in place* (starting, some, significant): What role has internal audit played during the development of your organization's automation program?



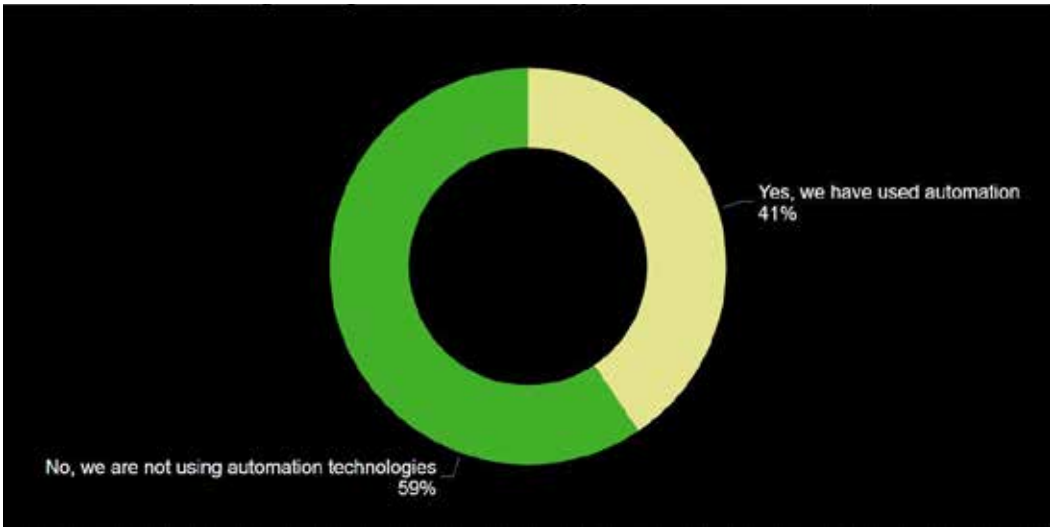
For responding organizations that had *some level of automation in place* (starting, some, significant) and where internal audit *is consulted and informed or is planning a review* of automation capabilities: Where internal audit has or plans to review the automation capabilities, what is the focus of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



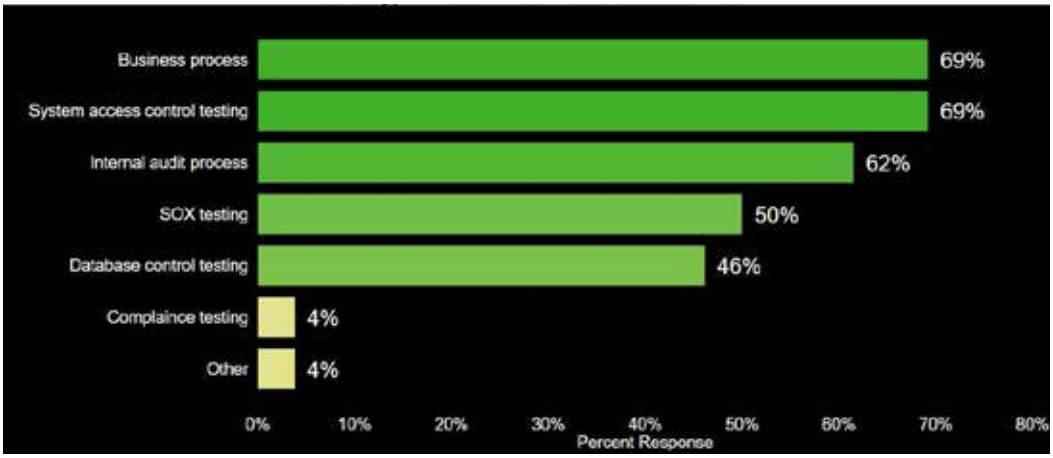
Where IA is consulted & informed or planning a review of automation capabilities: Is the audit of automation technology and processes part of your ongoing annual internal audit plan?



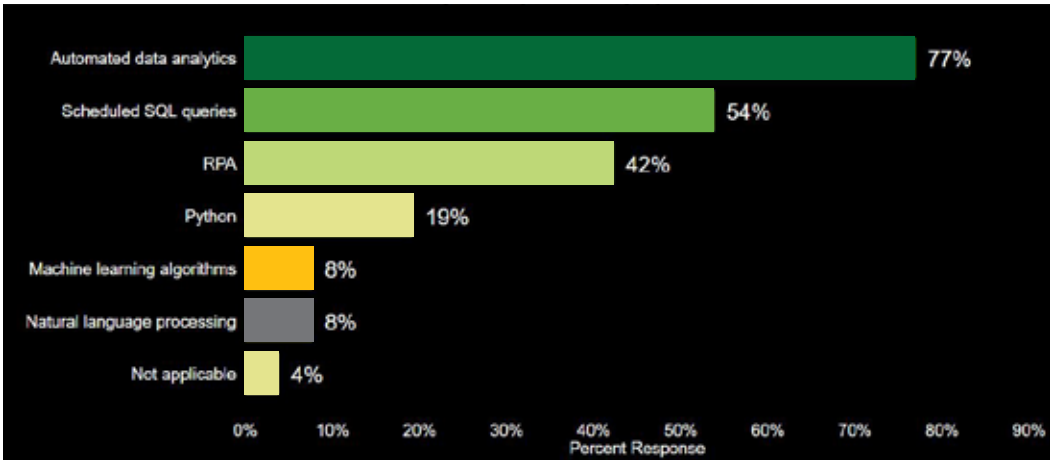
Is the audit planning or using automation technology within the internal audit scope of work?



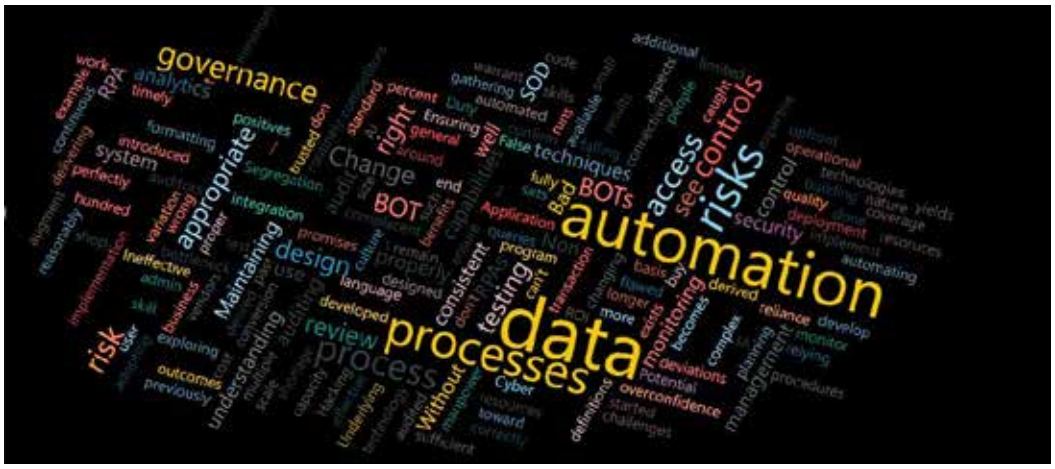
What type of audits have used automation?



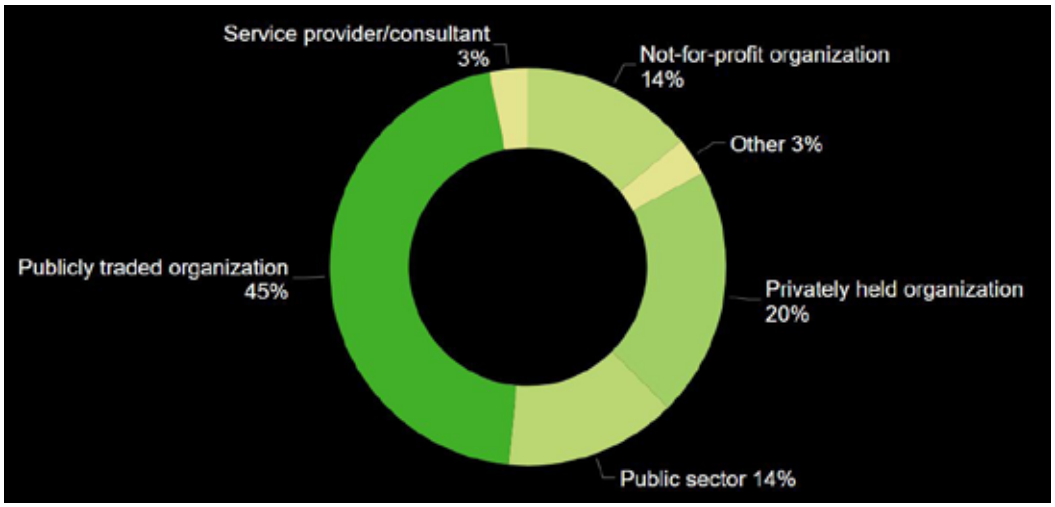
What automation technologies are you leveraging within internal audit?



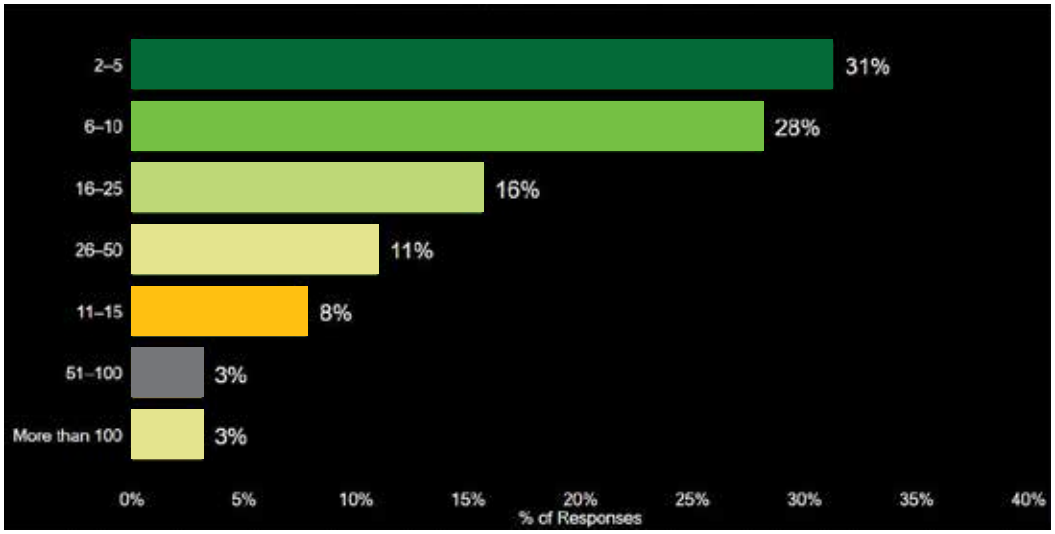
What are the risks that you see from introducing the automation technology to your organization? Repetition factor = 1



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