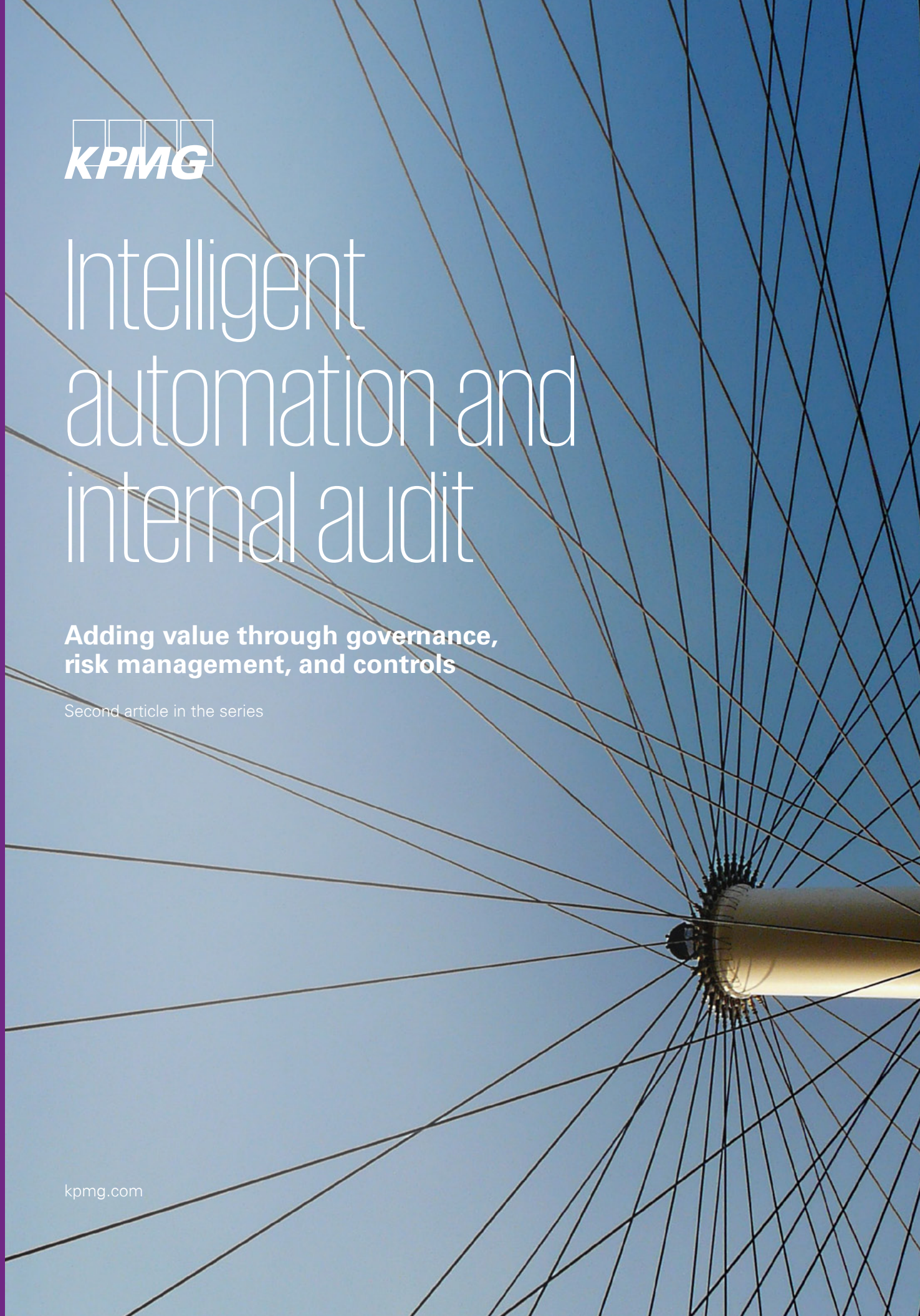


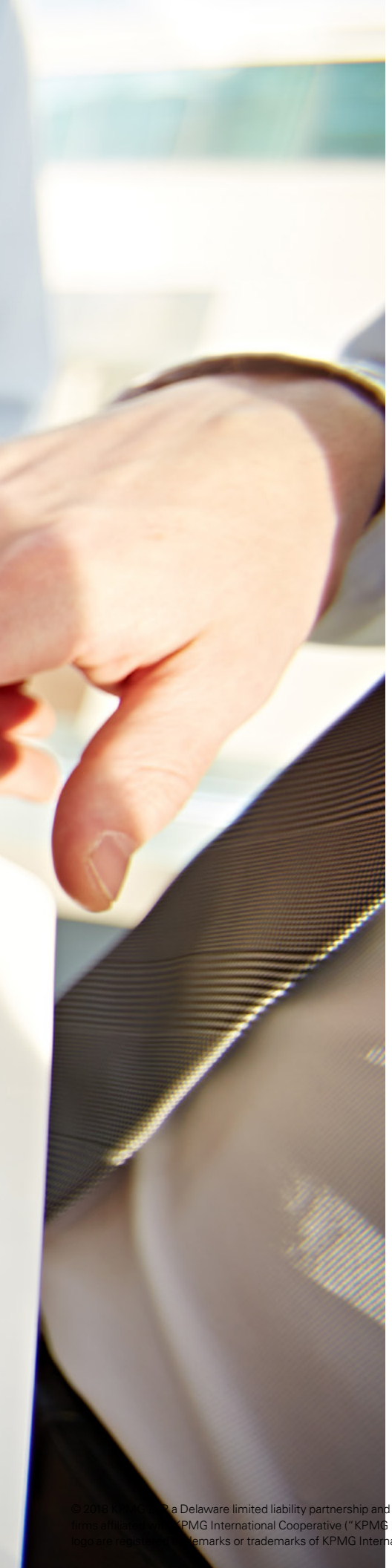
KPMG

Intelligent automation and internal audit

Adding value through governance, risk management, and controls

Second article in the series

kpmg.com



Contents

Governing intelligent automation across the enterprise

Intelligent automation does not just bring new opportunities for lower costs and greater efficiencies; it also brings new risks.

As we described in our first article on Intelligent Automation and Internal Audit, "Considerations for assessing and leveraging internal audit," intelligent automation can do more than automate simple or repetitive procedures. Using big data, predictive analytics, process robotics, cognitive systems, natural language processing, machine learning, and artificial intelligence, advanced automation can perform knowledge work too.

Just as this astounding power can change how an organization does business, it also creates new challenges for the control environment, such as how to supervise computer programs that can learn from experience and modify themselves. Internal audit can help the organization understand, evaluate, and assess the new governance, risk management, and control considerations associated with an intelligent automation program.

Will your internal audit department understand the new risks associated with automation and be able to provide insights and assistance throughout the automation journey?

Key opportunities for internal audit within intelligent automation initiatives include the following:

01 **Internal audit can help integrate governance, risk, and controls considerations throughout the automation program life cycle as an organization establishes and implements its program.**

02 **Internal audit can help the organization identify opportunities to embed automation-enabled control activities within the impacted business processes and functions.**

03 **Internal audit can capitalize on intelligent automation innovations to increase the efficiency and effectiveness of its own activities.**

New risks from new technology

Organizations that deploy intelligent automation—as most will, sooner or later—have to consider questions about **governance and risk**, beginning with ownership. The business, IT departments, centers of excellence, and vendors all have a stake in intelligent automation programs. As a result, programs need to establish unified oversight of key performance indicators (KPIs), key risk indicators (KRIs), and risk mitigation and risk acceptance processes. This oversight helps form the framework for developing and managing bots[1]—the computer programs that are at the heart of intelligent automation—in a manner that supports the program's strategy while maintaining consistency and security.

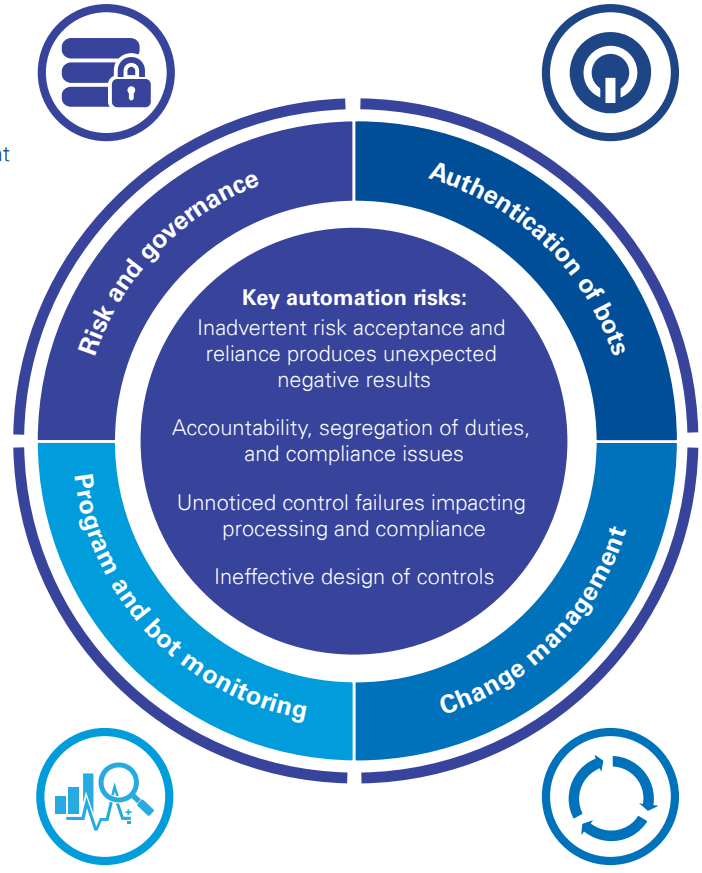
Most organizations know how to assess their employees' competencies to gain confidence in their performance. But do they know how to build and assess the competencies of bots, particularly those that use artificial intelligence for more complex tasks? **Controls** are needed to validate that bots continue to perform as intended and are maintaining the completeness, accuracy, and integrity of data. To be effective, these controls need to be considered and consistently applied throughout the automation program life cycle (see Figure 1).

Figure 1: Automation program life cycle

[1] A *bot* was originally short for robot but now specifically refers to computer programs that run automatically. A simple early example is a Web crawler, which scans Web sites to look for and record information, but far more sophisticated examples, powered by artificial intelligence, are becoming more common.

As organizations implement intelligent automation programs, there are common pitfalls related to the emerging governance, risk, and control considerations related to such programs, as illustrated in Figure 2. Understanding these potential pitfalls—and why they matter to the success of the program and organization—can help the organization develop a plan to mitigate, or even prevent, such issues.

Figure 2: Common risk pitfalls of intelligent automation programs



- Undefined ownership of intelligent automation program
- General lack of oversight of risk
- General lack of program oversight
- Lack of consistent and secure development and management of bots

- Lack of controls for proper ownership of bots and effective integration with applications
- Lack of bot accountability relating to security, privacy, and compliance requirements
- Improper bot access provisioning and password management

- Varying skill levels and inconsistent developer training
- Lack of automated alerting tools for error handling and resolution
- General lack of controls around "Is the bot doing what it is supposed to be doing?"

- Lack of formal process for assessing how source application changes affect bots that access them
- Lack of a formal and consistent process for requesting and implementing changes to bots
- Lack of segregation of RPA development and production

For more information and considerations regarding how implementing an intelligent automation program impacts the enterprise risk profile and examples of process (or bot) level risks, read about Intelligent automation takes flight.

Consulting and assurance services: Internal audit's dual roles

With the right skills and resources, internal audit can help identify new risks, integrate and improve governance, and assess controls related to intelligent automation. Internal audit can take a two-pronged approach to working with the organization by providing both consulting and assurance services, depending on the needs of the organization at the given time.

1. **Consulting services** provide "advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training."[2] The "client" for consulting services can be any key stakeholder, such as the business owner, process owner, control owner, etc.
2. **Assurance services** provide "an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements."[3]

If your organization is just beginning its intelligent automation program, internal audit may begin with an "in-flight" or "preassurance" assessment to provide valuable insights while the program or a particular use case is still being established (i.e., consulting with the second line of defense as they set standards for the program). If your organization is further along in its automation journey, internal audit can expand its focus to include assurance activities to audit the overall program and effectiveness of the related controls and processes.

[2] The Institute of Internal Auditors, Standards Glossary

[3] Ibid.

Adding value at every stage

To better understand internal audit's opportunities to help the organization throughout its intelligent automation program, we will look at examples of where internal audit can add value through consulting or assurance services during each stage: plan, build, run, *and* monitor.

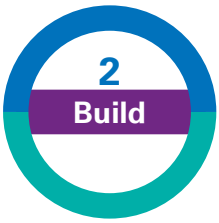
Whether the organization is getting ready to deploy an intelligent automation program or is embarking on a specific use case, the risk profile and related risk appetite should be assessed for each. In the planning stage, the organization should understand the organizational, functional, industry, regulatory, and compliance requirements that will inform the governance program.

Consulting services example reviews

- Business case for change and bot use case
- Strategy and road map
- Solution platform(s) and target architecture, including alignment with existing systems
- Vendor selection and pricing

Assurance services example assessments

- Adoption of policies and procedures
- Process and technology standards
- Vendor performance and billing



As work begins on delivering intelligent automation solutions, the organization should launch a governance framework early in the solution development life cycle (SDLC) to enable consistent, effective risk management. This framework should integrate controls, policies, procedures, training, toolkits, templates, and accelerators to support the build. As bots are developed, controls should be in place regarding coding practices, secured authentication, data access, and interactions with other applications, to name just a few considerations. This stage should commence with thorough user acceptance testing of the bot performance.

Consulting services example reviews

- Business and technical user engagement
- Delivery quality and budget management
- Lessons learned (technical and functional) and implemented
- Risk identification and control design

Assurance services example assessments

- Application of the SDLC methodology
- Bot development, testing, and acceptance procedures
- Control design and operating effectiveness, including system configurations, identity access management, etc.
- Real-time system implementation

KPMG

As the organization begins to implement intelligent automation within its business activities, controls should be embedded into the day-to-day operations to monitor performance and effectiveness. These controls should identify, evaluate, mitigate, and, when appropriate, accept risks. To avoid common errors of the digital age, such as ineffective logging, monitoring, and analytics capabilities, organizations should establish automated tools to identify and resolve errors and analyze trends. New continuity risks may also arise, as system outages, for example, could find bot-dependent organizations without the human resources and skills to maintain critical functions manually.

Consulting services example reviews

- Transition of intelligent automation use cases into operations
- Definition and embedding of KRIs and controls
- Design of performance modeling and monitoring

Assurance services example assessments

- Operational performance and quality
- KRI effectiveness and reporting
- Realization of benefits and sustainability
- Control design and operating effectiveness

With an intelligent automation program up and running, the organization and internal audit should seek to continuously improve performance and manage known and emerging risks. Activities include monitoring KRIs; conducting periodic audits; championing better practices in governance, risk management, and controls; and collaboratively identifying opportunities for improvement.

Ideally, internal audit will contribute to the intelligent automation program life cycle from the start. However, even if internal audit enters when the program is already up and running, it can help align risk management and controls with the organization's risk appetite, maintain that risk position, achieve compliance, and identify improvements.

Consulting services example reviews

- Intake management of current and future use cases
- Stakeholder engagement
- Risk appetite evaluation

Assurance services example assessments

- Real-time auditing/monitoring
- Management of and sensitivity to risk appetite
- Effectiveness of the continuous improvement process
- Emerging risk identification and control design

For new and mature programs, a thorough review

Whether your intelligent automation program is just beginning or is already up and running, internal audit consulting or assurance services can add value to the program. If not well-designed and controlled, automation is risky. For example, you do not want your organization to be the next to make headlines for data breaches or system failures.

An effective review by internal audit will cover six areas:

1. **Strategy.** Look for a clear vision of the intelligent automation program's goals and evidence that indicates management understands and supports that vision. Business cases should include a value assessment and measurable KPIs. Technology strategies (host vs. cloud) and vendor strategies (build vs. buy) should align with the program's overall strategy.

2. **Technology.** Teams must effectively apply SDLC controls to intelligent automation development activities and assess the ongoing auditability of processes and control activities that intelligent automation will perform. Teams should also consider how automation is changing the overall technology environment and infrastructure, as new servers, tools, third parties, and integration options are developed. Controls should be designed to cover the supporting infrastructure as well as the bots. For example, if there is a server failure, how does that impact critical processes performed by bots, and is there an appropriate disaster recovery plan in place?

3. **Process.** You do not want to automate an ineffective process. Standardizing and optimizing processes, and the related controls before automation, may open doors to further automation potential and a greater ROI. For example, if manual processes performed differently in various business units can be standardized, the automation use case can be extended to all business units with minimal additional costs. Before deploying automation, check that the right teams are evaluating the process, capturing its risks, and preparing to manage those risks. Business requirements, including compliance requirements and variants from the standard process, must be documented in detail.

4. **People.** Intelligent automation requires changes to capabilities and skill sets: (1) Experienced personnel will be needed to develop, troubleshoot, support, and improve the new technologies, and (2) in business functions where intelligent automation is implemented, the existing workforce will need to shift skills from transactional processing to more critical thinking, problem solving, issue resolution, and research skills. Organizations should have a plan to redeploy or acquire talent to meet these needs, as well as implement change management and communication plans to address transitions within the workforce.

5. **Controls.** Identify the financial, operational, and compliance controls that either can be automated as part of the solution or will be impacted by it. Examine procedures to validate the completeness and accuracy of all information processed through intelligent automation and assess controls designed to identify when a bot fails to work as it should.

6. **Program management and governance.** Review whether roles and responsibilities in deploying, monitoring, and owning intelligent automation processes have been well-defined, with the right stakeholders involved at each stage. Examine processes for vendor selection, approval, and oversight and for technology oversight, including intellectual property ownership. Evaluate governance activities to determine if the expected value was realized and that the program continues to scale to meet the strategic business objectives.

KPMG

Key takeaways

Intelligent automation requires new considerations for governance and controls to manage risk. Internal audit should work with the organization to:

1. Understand how automated and increasingly intelligent applications impact the organization's risks and controls
2. Establish a governance framework suited to an "automation-driven" environment
3. Review the design and effectiveness of that framework to identify gaps and possible improvements.

Through various consulting and assurance services, internal audit can provide value and partnership throughout the intelligent automation journey. Proactively supporting the organization's governance, risk management, and control activities helps inform and enable that journey with internal audit's unique insights.

Stay tuned for the final two papers in this four-part series on intelligent automation and internal audit:

— **Part three:** Learn how internal audit can help identify opportunities to embed automation-enabled control activities into business processes and functions on the intelligent automation journey.

— **Part four:** Explore how internal audit can increase its own value by capitalizing on intelligent automation within the scope of daily internal audit activities.

KPMG: Intelligent Automation Risk & Governance

Our focus is on helping to ensure that our clients' intelligent automation program, platforms, and bots are effectively governed, risk is managed, and controls are properly contemplated and integrated into the solution. Our work helps enable effective compliance with internal controls and assurance requirements (i.e., internal audit, IT policies, etc.) and external requirements (i.e., SOX), as well as leading practices related to data security and privacy, change management, and processing integrity, auditability, etc., across various phases of intelligent automation transformation, including strategy, delivery, and operations.

To learn more about how KPMG can help your organization enable intelligent automation solutions while mitigating risk, please visit our Web site.

Contact us

Deon Minnaar
Internal Audit and Enterprise Risk Service Network Leader
T: 212-872-5634
E: deonminnaar@kpmg.com

Michael A. Smith
U.S. Intelligent Automation Leader (IA and SOX)
T: 214-840-6019
E: michaelasmith@kpmg.com

Martin Sokalski
U.S. Intelligent Automation Leader (Emerging Technology Risk Services)
T: 312-665-4937
E: msokalski@kpmg.com

Contributors

Special thanks to authors Michael Smith, Martin Sokalski, Paige Woolery, and Karen Uihlein and writer Laura Bubeck.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia