KPMG

Intelligent automation takes flight

Risk and governance will help you safely land your automation goals

kpmg.ie

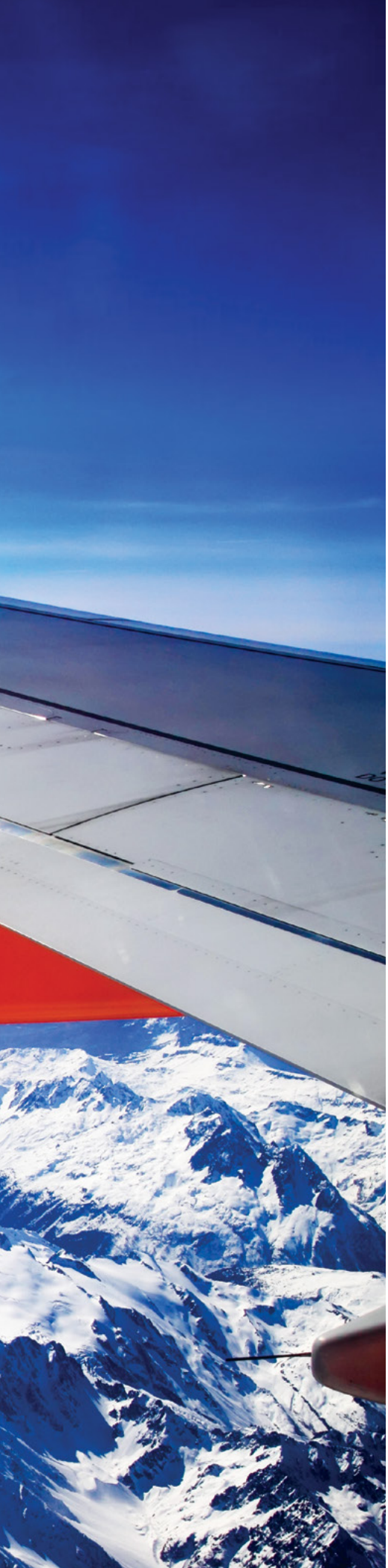


Table of contents

Avoiding turbulence on your intelligent automation journey

Intelligent automation is changing the world of business, right before our eyes. This new wave of advanced technologies has the power to exponentially increase enterprises' speed, scale, quality and precision, drive never-before-seen levels of operational efficiency, and both complement and augment human skills.

The rampant digitization of labor means traditional ways of operating business are becoming obsolete. Smart machines now perform activities, and even make decisions, previously left exclusively to humans—and they do it faster, more accurately and at far greater scale.

That means the days when employees clock in to work just to repeat mundane, manual tasks over and over will soon be a distant memory. According to recent KPMG research, 89 percent of technology leaders are maintaining or ramping up investment in innovation, including in digital labor.[1] Other KPMG research found that artificial intelligence (AI), cognitive computing and robotics are among the top technologies that will drive business transformation.[2]

What is intelligent automation?

Intelligent automation is the continuum of technologies companies use to automate both transactional and knowledge-based business processes. Today, smart bots create reports, assist auditors, analyze tax information, conduct legal research, advise on medical treatments, provide investment guidance, and detect security breaches. Examples abound from every sector: the smart assistant on your mobile phone that tells you today's weather, the customer service chat bot that helps you submit an insurance claim, and the feature on your car that lets it park itself.

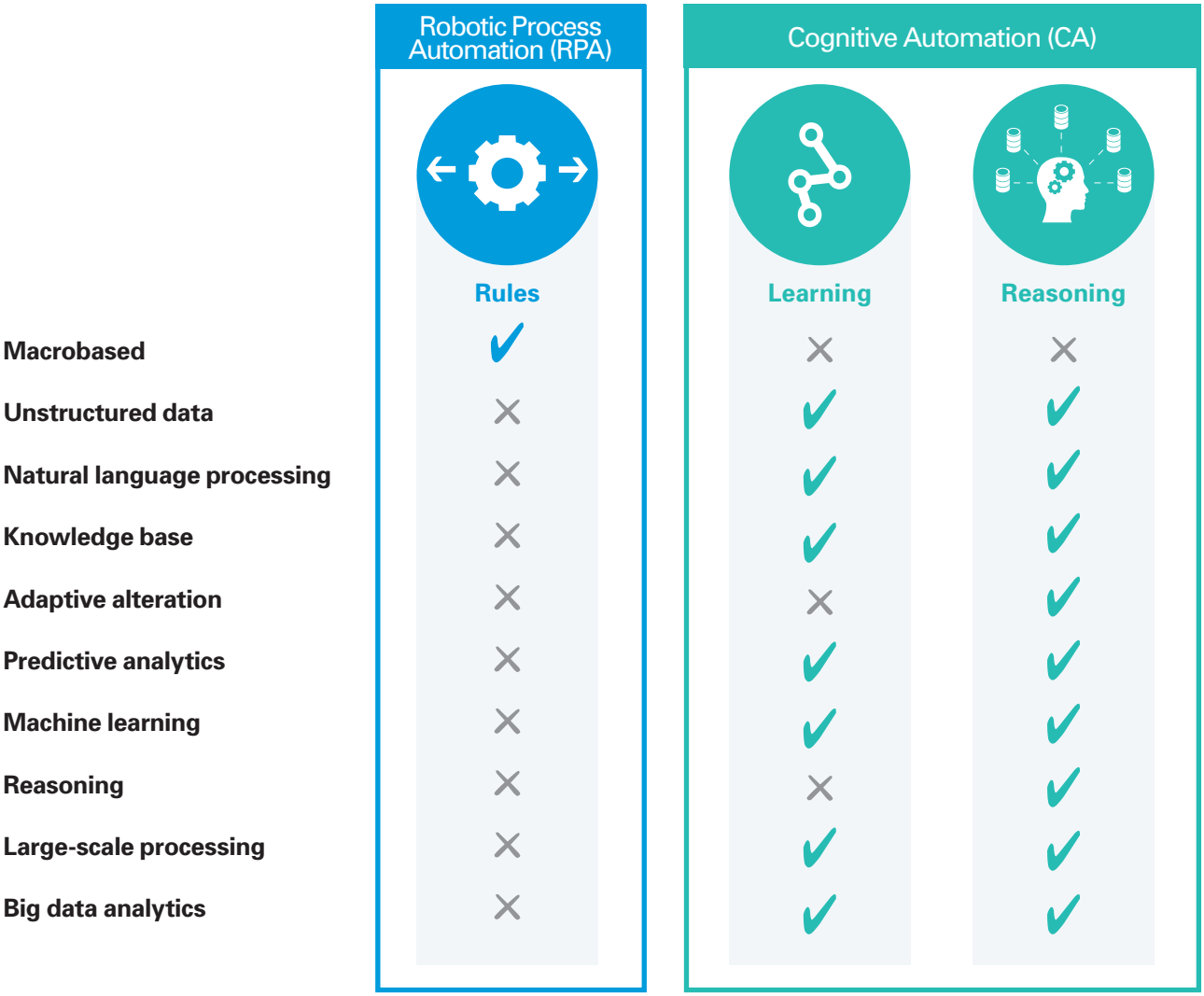
Intelligent automation is not just one technology—it's a range of tools with different advanced capabilities. At KPMG, we categorize these tools along a spectrum, ranging from robotic process automation (RPA), which automates very rudimentary processes such as transaction processing, to cognitive automation, which mimics human activities such as hypothesizing, reasoning, and deriving insights from masses of unstructured data.

1 CIO Survey (KPMG International and Harvey Nash, 2017)

2 Changing Landscape of Disruptive Technologies (KPMG International, 2017)

KPMG

KPMG categorizes intelligent automation into three classes:



Avoiding turbulence on your intelligent automation journey

Given its clear benefits and countless use cases, it's no wonder intelligent automation has become a mission-critical initiative. The race is on and there is simply no turning back. But as a leader in one of the many organizations considering a takeoff—or already in flight—you know embarking on such a broad and important digital transformation project is no time to throw caution to the wind.

That's where intelligent automation risk and governance comes in. A well-designed risk and governance function helps ensure your intelligent automation program avoids a turbulent flight or a crash landing—that any and all risks associated with the digital transformation are effectively identified, evaluated and mitigated (or in some cases, accepted).

In this paper, we'll examine:

1. **What happens when intelligent automation isn't appropriately controlled and managed**
2. **Where risk and governance fall in the intelligent automation ecosystem**
3. **A framework for integrating risk and governance into the intelligent automation program**

"Rates of adoption of intelligent automation with all industry verticals and business functions jumping on the bandwagon are at an unprecedented level."

- Martin Sokalski, Principal, Emerging Technology Risk

"Companies will need to evaluate desired business outcomes, level of financial investment and complexity of task/process to help determine which classes of intelligent automation addresses their needs while understanding the risk implications of automation."

- Kelly Combs, Manager, Emerging Technology Risk

When bots go wild

Can an enterprise lose control over an entire army of bots?

Can the intelligent automation tools your business relies upon run amok, performing unintended and potentially damaging actions?

Yes. Without a proper approach to managing risk, these two hypothetical scenarios can easily move from science fiction into dark reality. As with any disruptive technology, the rapid adoption of and reliance on intelligent automation is transforming the enterprise risk landscape, exposing businesses in new ways, creating more vulnerabilities, and increasing the level of complexity. Whether in a single function or across the enterprise, implementing intelligent automation creates not only technology risk, but also regulatory risk, financial risk, operational risk, and reputational risk.

Yet, a significant number of organizations are not thinking about intelligent automation's potential risks and governance considerations. KPMG's 2017 Information Technology Risk Management Survey found that one-quarter or more of organizations have adopted cognitive computing **(25%)**, robotic process automation **(32%)**, or artificial intelligence **(34%)**, yet failed to include these emerging technologies in IT risk assessments.[1]

Below we highlight a few of the unique risks your intelligent automation could expose your business—and your customers—to:

Business disruption

Skill gaps. Inconsistent developer training. Lack of change management processes. Insufficient cybersecurity. Lack of or ineffective controls. A slew of factors could create an unstable bot environment and increased bot failure rate. And when your bots stop working, so does your business.

Consider:

1. How will you design your automation program with appropriate risk considerations in mind to reduce the opportunity and impact of critical bot failure?
2. How will you ensure you're able to recover from a business disruption impacting your automation platform, especially when it affects bots used for mission-critical processes?
3. How will you manage changes to the automation environment while maintaining integrity, functionality, compliance and proper controls?

1 ITRM Disruption Survey, (KPMG LLP, 2017)

KPMG

Non-compliance

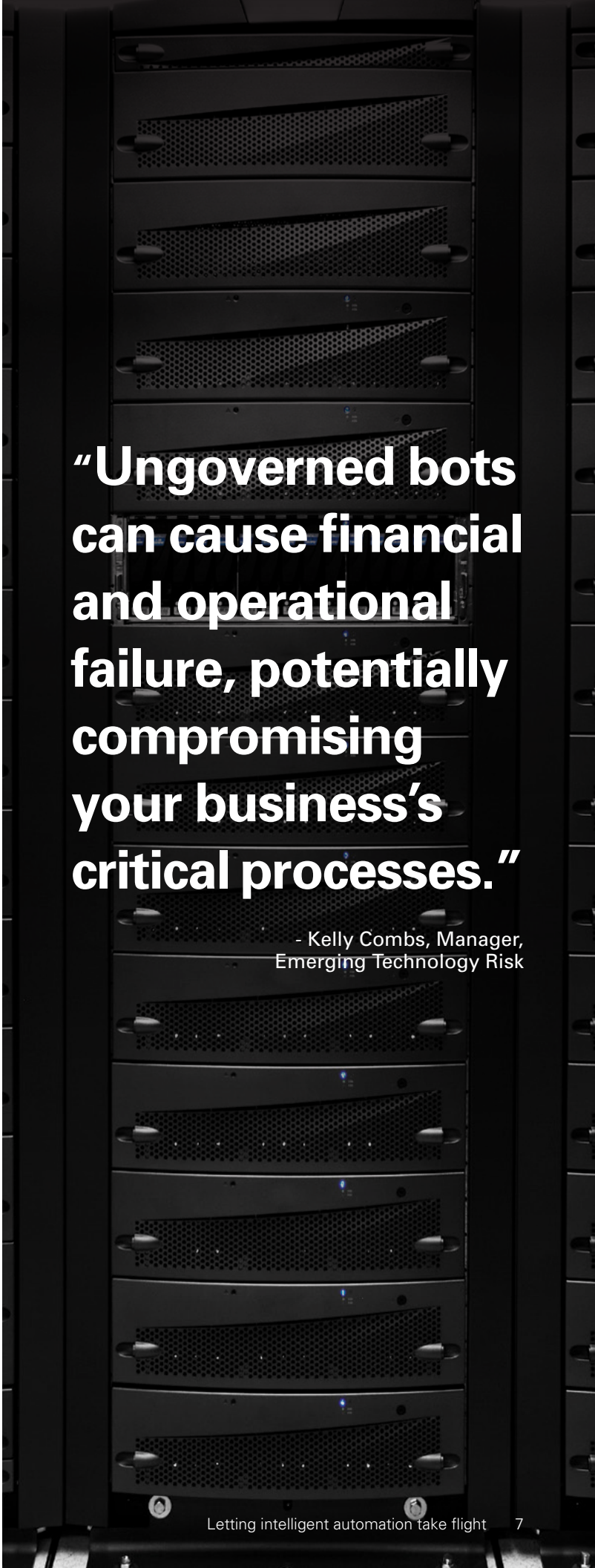
A lack of well-defined guidelines around your automation program can prevent you from meeting governance, risk, controls and compliance requirements. This could damage your relationships with partners, auditors, and regulators. Big fines could ensue. Or non-compliance can lead to a program that lacks stability and is subject to operational failures. Always remember that organizations deploying intelligent automation programs may need to provide assurance that they are abiding by relevant regulatory and compliance guidelines. Identification of impacted internal and external compliance requirements should be one of the first considerations when implementing an intelligent automation program.

Consider:

1. How will you maintain data security and privacy during storage, processing and transmission?

2. How will you secure bots from unauthorized access to prevent data leakage, intellectual property theft, or introduction of malicious code into system processing?

3. How will you ensure the processing of each transaction and activity has an acceptable level of confidence and integrity, as required by compliance?



"Ungoverned bots can cause financial and operational failure, potentially compromising your business's critical processes."

- Kelly Combs, Manager, Emerging Technology Risk

When bots go wild

Business and IT control failures

The lack of proper access and authentication controls for bots creates issues with accountability, segregation of duties and potential for unauthorized transactions. Poor controls integration and monitoring may also result in unnoticed control failures. Depending on which controls are at fault, you could face major problems with security, integrity, compliance, or even business continuity. Proper access provisioning, secured authentication, segregation of duties and secure application integration need to be enabled within the program. A lack of these security and privacy considerations may lead to data loss and cause operational and reputational harm. In addition, data security and privacy requirements should be built into the design of bots, including appropriate logging and auditing capabilities.

Consider:

1. How will bots be provisioned and what access will they have?
2. How will you create appropriate levels of transaction traceability to audit bot activities?
3. How will you ensure automated controls are performed completely and accurately, especially those subject to control testing?
4. How will you ensure bots don't have too much access, allowing them to override existing controls?

A lack of these security and privacy considerations may lead to data loss and cause operational and reputational harm.

...algorithms that are not regularly audited, monitored, tested and managed can be fed the wrong data, leading to skewed or biased results that only worsen over time...

KPMG

Unintended actions

In cognitive environments—which rely extensively on training data and machine learning—algorithms that are not regularly audited, monitored, tested and managed can lead to skewed or biased results that only worsen over time—especially if the automation is unable to detect malicious or incorrect input. Ultimately, the system will make inaccurate decisions, whether that means giving a customer bad investment advice, developing an incorrect marketing or credit bias for a segment of clients, or drawing the wrong conclusion about the viability of a new product launch idea[1,2] (see sidebar).

Consider:

1. How will you staff teams with the right talent to pilot, build and train cognitive solutions?
2. How will you prevent data manipulation within the cognitive system?
3. How will you regularly manage cognitive algorithms to ensure the accuracy and integrity of AI-driven decisions?
4. How will you monitor the algorithm's conclusions and identify degradation of the algorithm, which may require retraining?

1 When Not to Trust the Algorithm (Harvard Business Review, October 18, 2016).

2 There's a big problem with AI: It's creators can't explain how it works (Technology Review, May 12, 2017)

Bots behaving badly

Cognitive systems expose businesses to unique risks that many don't anticipate, let alone plan for. One company learned that the hard way when it created a Twitter chatbot that uses artificial intelligence to engage with other Twitter users through "casual and playful conversation." Unfortunately, Twitter users started tweeting inflammatory comments to the chatbot, which ultimately started repeating these sentiments back to users.

Source: Microsoft Created a Twitter Bot to Learn From Users. It Quickly Became a Racist Jerk. (The New York Times, March 24, 2016)

Addressing automation risk

The what

These risks described are very serious. They clearly demonstrate the critical need for strong risk management and governance of your intelligent automation program.

But as you begin to implement intelligent automation, where and how should you start addressing risk? That's the big question.

Before understanding how to approach risk and governance, you first need to understand the three core components of the intelligent automation ecosystem: technology, process and people.

Risk & governance

Technology

- Solution architecture (hosting, platforms, applications, interfaces) and underlying infrastructure
- Integration with existing systems and applications
- Bots and algorithms
- Data that flows through technology that support the overall business process
- Network, services and devices that allow for connectivity

Process

- Functional business processes and use cases that will be transformed via automation
- Governance, policies, methods and accelerators that govern and enable intelligent automation
- Risk management, change management, issue tracking, performance and benefit management, financial management, etc.
- Communication, change enablement and training
- Delivery models (centralized, hybrid, and distributed)

People

- Cultural shift and changing behaviors
- Talent management and workforce shaping
- Organizational structure and roles and responsibilities
- Workforce impacted by automation
- Stakeholders setting strategy, building, operating and supporting intelligent automation platforms
- Functional technology and process owners and governance committee overseeing automation

KPMG

As with any process that touches many different functions throughout an enterprise, it is critical that you effectively integrate risk and governance across the entire automation ecosystem, with a dedicated function responsible for overseeing the smooth operation of technology, process and people that make up the program.

In fact, we submit that an overarching risk and governance function is one of the keys to realizing the business benefits of intelligent automation. A risk and governance function will enable repeatable policies and procedures that allow you to scale along your automation journey and mitigate program level risks.

The risk and governance function should:

- Govern people, process and technology at the program and individual bot level
- Develop and deploy automation policies, procedures, standards and guidelines
- Provide risk oversight, direction and authority for the intelligent automation program, including risk identification and monitoring, evaluation, mitigation, and, in some cases, risk acceptance

As you begin to implement your intelligent automation program, where exactly does risk and governance come into play? Everywhere. The risk and governance function should inform, oversee, enable and guide every part of the program—from strategy to delivery to operations—because things could go wrong at any point.

Addressing automation risk

The what

"Bots should be developed to a standard that is secure, scalable, and sustainable and can be re-used."

- Martin Sokalski, Principal, Emerging Technology Risk

Strategy

The risk and governance function should play a key role in defining and evaluating the automation platform and a pipeline of automation use cases. Examples include defining risk profile and tolerance based on organizational, functional, industry and regulatory landscape and compliance requirements.

Strategy risks:

- Inadequate identification and mitigation of risks introduced by the intelligent automation
- Intelligent automation program not aligned with overall business objectives
- Lack of appropriate involvement from stakeholders across engineering, security, privacy and legal
- Lack of implementation road map for connected features

Delivery

The risk and governance function should help enable a process of secure and scalable bot development, quality assurance and controls integration. Examples include integration of risk management in the delivery of solutions through deployment of training, toolkits and templates to effectively identify, evaluate and mitigate risk associated with initial development and delivery of bots and the ultimate expansion of the intelligent automation program.

Delivery risks:

- Security and privacy controls considered as an after-thought during product development cycle
- Agile and rapid development moves faster than risk and controls
- Software development and ongoing support is not a core competency of the organization
- Integration with other devices exposes vulnerabilities

Operations

The risk and governance function should enable effective program monitoring including key risk and performance indicators and value-driven data analytics. Examples include establishment of key risk indicators (KRIs) for ongoing operation of the program.

Operations risks:

- Inadequate risk monitoring and reporting can result in inadvertent reliance and risk acceptance.
- Without appropriately capturing and analyzing data from the automation program, intelligent automation may not provide the business value and risk optimization.
- Evolving cybersecurity threats related to hacking, malicious software, and other system vulnerabilities

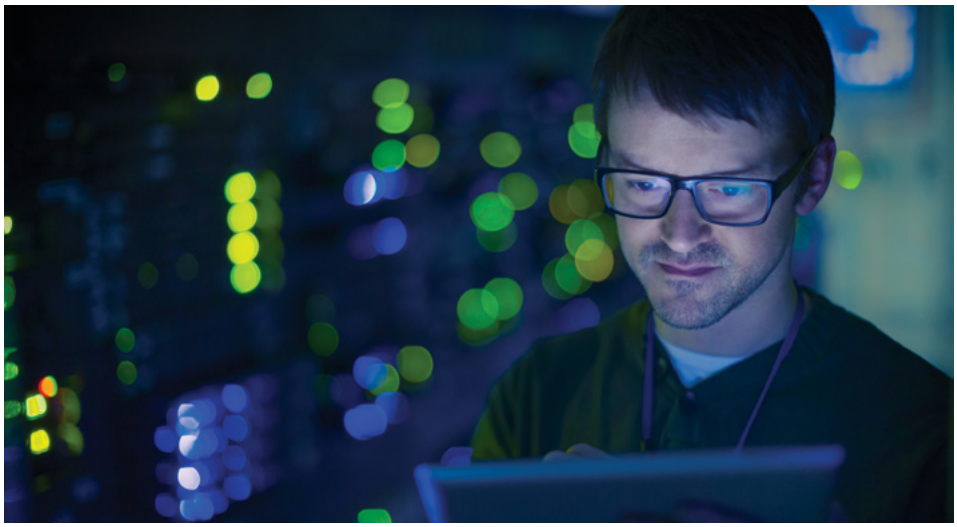
KPMG

Addressing automation risk

The how

Of course, it's easy enough to talk about integrating risk and governance throughout the automation journey at the theoretical level. Actually doing it is another matter.

So let's get practical. There are tangible actions your risk and governance function can take as you are strategizing, delivering and operating your bots to keep the intelligent automation program under control. We have broken these actions down across the three core phases, or activities, that make up your intelligent automation implementation program: **Plan. Build. Run.**



Plan

Incorporating governance, risk management and compliance

- Define your risk appetite, requirements and scope
- Establish risk management guidelines to identify, evaluate, monitor, manage and mitigate risk
- Evaluate risk in Use Cases and "What Could Go Wrong" scenarios
- Establishing key risk indicators and controls
- Design a risk and governance framework

Build

Standing up a governance function

- Perform due diligence review of solution configuration
- Test platform controls
- Develop risk templates, registers and toolkits to monitor risk
- Establish cross functional governance charter with policies
- Enable stakeholders through training, including steering committee, CoE, controls owners, and developers

Run

Support on-going execution of CoE and compliance program

- Establish control ownership, test procedures and monitoring process
- Utilize risk templates, registers, toolkits as part of program operation
- Monitor automation KRIs
- Report on compliance metrics to key stakeholders
- Collect and analyze data to optimize the automation program

Plan:

Understand your use case scenarios

You're not implementing intelligent automation just to say you did it. You have a reason. It might be a financial motive, to reduce overhead or redundant costs. Or it might be an operational motive, to increase speed to market.

Whatever your motivation, your organization might be ready to accept certain risks to achieve its desired goals. Or you might not. Maybe you are in a highly regulated industry, like healthcare or financial services. Or you are looking to automate a process that is subject to lots of rules and requirements, like SOX or HIPAA, or that involves highly sensitive data (see sidebar).

To effectively manage risk, you must have a strong handle on all of the above. That's why understanding the nature, impact and complexity of your automation program use cases—including the specific benefits you expect it to bring about—should be your starting point to managing risk. That way, your approach to risk and governance will align with the organization's risk appetite, tolerance and strategy.

Not all bots should be created equal

All intelligent automation programs must be sound from a risk and governance perspective. But some bots may demand stricter requirements and integrity checks than others, such as bots involved in especially complex or critical processes or bots that drive processes that are subject to intense regulatory scrutiny.

Design considerations for each bot should be driven by an early-stage risk evaluation, which drives the requirements for controls integration into the holistic program as well as each individual bot. Highly regulated industries such as banking, healthcare and insurance should also monitor regulatory and compliance issues on a regular basis to ensure the intelligent automation program remains compliant.

KPMG

Key action

Evaluate what impact existing or planned automation has on the enterprise in the context of opportunity as well as risk profile, controls and compliance requirements at the program and individual bot levels.

More tips for success

Consider who is responsible for prioritizing and approving automation initiatives, and what department will reap the benefits to avoid conflicting business priorities, resource constraints, introduction of risks and inability for IT and the business to reach full automation potential.

- Leverage both business and IT stakeholders to weigh in on the potential automation use cases and define the program's risk appetite
- Perform a due diligence review of the automation platform to identify key risks, implement policies and procedures, select a vendor platform, understand technical requirements and address security concerns.
- Align technology platforms with the strategic vision of the company to avoid investment in multiple platforms with overlapping capabilities, or insufficient system functionality and agility. The absence of a scalable platform for automation expansion can lead to internal demands that exceed system functionality, potentially introducing integrity and security concerns.
- Assign roles and responsibilities for key activities in the automation implementation journey, especially when working with third parties (see sidebar).

Should you outsource automation?

Many business process outsourcing firms (BPOs) are now bringing automation solutions to contracts as a means to provide a lower cost solution, evolve their business models, and bring innovative ideas to their clients. If your company is looking to introduce automation with a BPO provider, consider the following from a risk perspective:

- Does your existing BPO contract make clear which party is responsible for controls and risk?
- Does your contract allow for rights to audit and require service organization control reporting?
- What technical requirements are you required to bring to the table to enable the automation?

Build:

Your platform is live. Now what?

It's not sufficient to just perform an initial risk review over the intelligent automation platform. Risk needs to be embedded from the beginning, implemented in the build stage and monitored on an ongoing basis. As your solution scales, risks can change. As the technology evolves and enhances, so may your risk exposure.

At this stage, your risk and governance function will be responsible for ongoing monitoring of the intelligent automation program. The function should perform initial due diligence and risk reviews of automation solution, design and implement platform controls, and begin educating stakeholders about their roles and responsibilities for automation risk management. In addition, the function should establish processes for reviewing, approving, credentialing, deploying, managing and decommissioning bots.

Key action

Unleash the risk and governance function to help inform and continuously guide the intelligent automation program strategy, delivery and operations.

More tips for success

- Establish a cross-functional governance charter with formalized policies and processes.
- Provide risk and governance tools, accelerators, and training to developers, the IT production support team, and the control owners.
- Enable management visibility into program issues and challenges and invite management to evaluate planned risk identification and mitigation activities.

KPMG

Run:

Support, monitor and evaluate

How do you continue to support the intelligent automation program from a risk and governance perspective? It comes down to operationalizing control ownership, capturing, analyzing and communicating relevant data, monitoring the integrity of automation processes, and tracking changes to the IT landscape that might impact bot performance. All of this should be enabled by the risk and governance function.

The risk and governance function should monitor key risk indicators (KRIs) and key performance indicators (KPIs) associated with the automation program and report them up to key stakeholders in order to optimize and scale up the program utilizing relevant data and analytics. It should establish business continuity and disaster recovery plans in the event of automation downtime. And it should also provide annual ongoing training to help ensure developers and production support have the appropriate skills and capabilities as technology platforms become more robust and prevalent.

Key action

Deploy intelligent automation-specific policies, standards, templates and accelerators to enable the enterprise to effectively and consistently identify automation opportunities, secure automation platform and bots, integrate relevant controls into bot build process to ensure compliance, and monitor the program.

More tips for success

- Develop tools and processes for continuous risk monitoring.
- Regularly review external compliance and regulatory requirements impacted by the intelligent automation program.
- Use dashboards to support the smooth operation of the automation program and identify issues and trends requiring people, process or technology change.
- Monitor and plan for changes to underlying technology systems.
- Put manual failover plans in place for business-critical automation if the technology fails.
- Embed "security by design" principles during bot development efforts and include penetration testing, software hardening and physical testing as part of bot quality assurance processes.

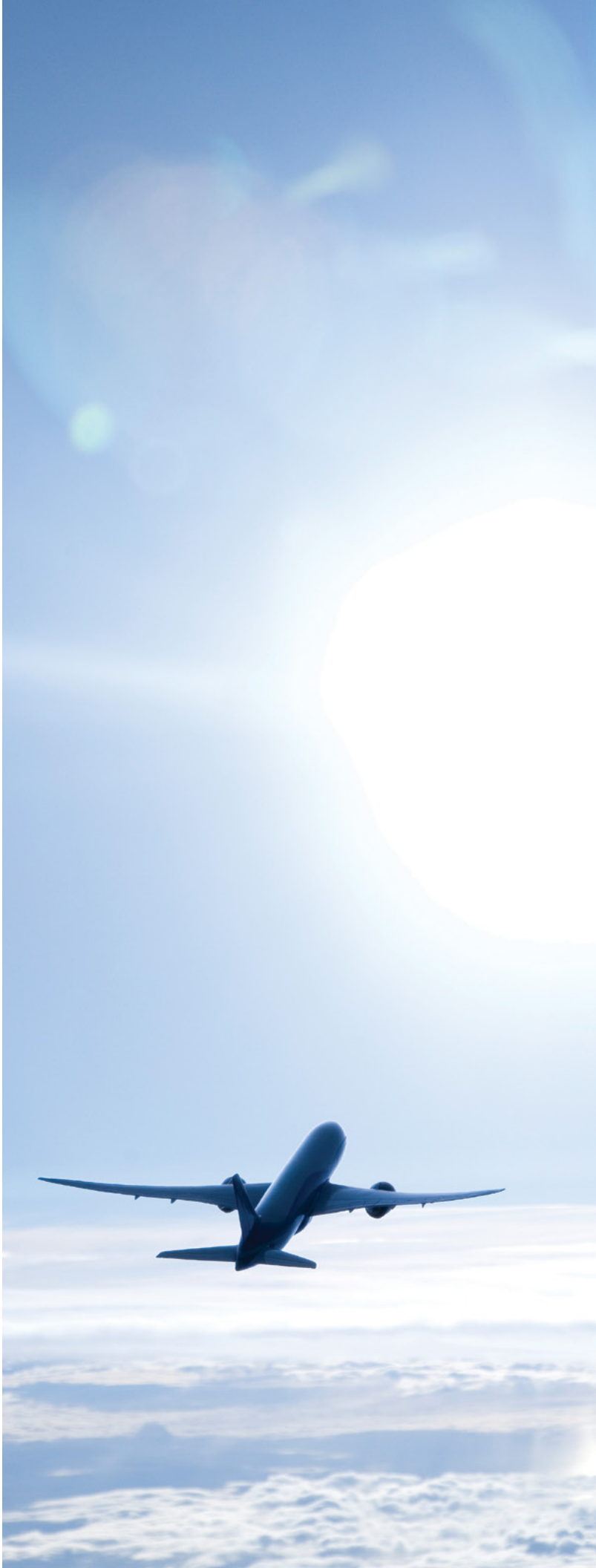
Safe travels

Given the tremendous potential value intelligent automation can bring to your business operations, it's tempting to let the excitement take over and fly freely ahead with implementation. But a successful intelligent automation journey isn't an uncontrolled flight; it requires proper controls and oversight. You need a comprehensive strategy to minimize the risks you might encounter along the way.

So before embarking, **think risk and governance.**

Use these questions to find out if you're ready for intelligent automation, from a risk and governance perspective:

1. Does intelligent automation expose you to enterprise, financial, operational or reputational risk?
2. How will you determine if the risks outweigh the rewards?
3. How will you manage the data, access and regulatory requirements associated with the automation program?
4. How will your technology platform ensure processing integrity, availability and business continuity, logging for trend analysis and error resolution, and agility to scale?
5. How will you govern the automation program and identify, monitor and mitigate risk throughout the automation journey?
6. How will you integrate risk considerations into the automation program strategy, delivery and operations?



KPMG

How KPMG can help

What we do

At KPMG we understand that technology is a key driver in enabling business and transformation. We are dedicated to helping clients who are implementing intelligent automation manage risk in order to achieve the value they expect from the program.

We have developed a comprehensive playbook for developing intelligent automation risk and governance functions and performing internal risk assessments. Our approach integrates risk considerations throughout the program lifecycle, and it grows with your automation program—without compromising innovation.

How KPMG can help

What sets us apart

1

We collaborate work with intelligent automation technology leaders. Since 2016, we have partnered with IBM Watson to leverage cognitive technologies to transform our own organization and the services we offer our clients. Automation Anywhere, IPSoft, Google and Microsoft are also part of our well-established ecosystem. These collaborations ensure we can provide the most value to clients, offering tailored solutions to deliver the most viable automation scenarios.

2

Our work is award-winning and recognized in the market. We were awarded Computerworld magazine's 2016 Data+ Editor's Choice Award. HfS recognized KPMG LLP in its 2016 Blueprint Report, naming KPMG a "High Performer" in the field of intelligent automation. And our technology partners recognize us too, with Alteryz presenting KPMG with its Innovation Award and Appian naming us Global Partner of the Year.

3

We support the full spectrum of intelligent automation, including strategy, identifying uses, process improvement, vendor and technology selection, architecture design, security, and people and change management. Our comprehensive offering covers the entire organization, including industry-centric verticals and horizontal functions.

4

We constantly watch the marketplace and technology. We invested early in process automation to become a pioneer in developing the right solutions for clients and ourselves. And our practice is constantly evolving, keeping pace as we monitor innovation and the adoption of new technologies.

5

We bring to bear some of the best and brightest minds in the field. The perspective we offer our clients is from aligning our global partners and professionals with notable technology skill sets. Industry-leading methodologies and processes also enable us to deliver services that help our clients navigate the challenges that come with adopting emerging technologies.

KPMG

About the authors

KPMG is a pioneer and leader in implementing intelligent automation solutions:

100+

intelligent automation transformations in progress

2,500+

intelligent automation professionals

200+

quality assurance/testing professionals

Clients in 155 countries, including

76%

of FORTUNE 500

Martin Sokalski

Intelligent automation Leader
Emerging Technology Risk Services
msokalski@kpmg.com

Martin Sokalski is the intelligent automation leader for KPMG's Emerging Technology Risk practice. He has more than 18 years of advisory experience helping organizations design new (and responsible) digital operating and governance models enabled by innovation and emerging technologies. Martin has advised clients on technology-driven innovation and transformation, risk management, governance, compliance, and IT audit and controls integration.

Kelly Combs

Intelligent automation Manager
Emerging Technology Risk Services
kcombs@kpmg.com

Kelly Combs is a manager in KPMG's Emerging Technology Risk practice specializing in robotic process automation (RPA) and intelligent automation programs. She has delivered a wide range of innovative and sound solutions to her clients, including intelligent automation risk assessments, implementations, use case identification, while integrating governance, risk, and controls into these emerging technologies and programs. She continues to support internal audit, risk management, IT, and business functions to realize the full benefit of intelligent automation.

Contact us

David Collins
Director
Management Consulting
KPMG in Ireland

T: +353 1 700 4282
E: david.p.collins@kpmg.ie

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

kpmg.ie