McKinsey & Company

Operations Practice

Managing the risks and returns of intelligent automation

As companies accelerate the adoption of automation and artificial intelligence, they need a better way to maximize the benefits of these new technologies while minimizing the risks.

by Federico Berruti, Akshay Phal, and Christophe Rougeaux

November 2021

The COVID-19 pandemic has pushed business digitization into overdrive. In surveys of top executives, more than two-thirds say their companies have accelerated their adoption of digitization and automation since the onset of the crisis (Exhibit 1). Many institutions (including banks, insurance companies, and other large corporate enterprises) are therefore deploying automation and AI solutions—a combination increasingly called "intelligent automation"—to optimize end-to-end business processes, automating not only tactical activities but also more complex prediction problems and decision making.

Intelligent-automation solutions can help to achieve efficiency and effectiveness gains, and support decision making by extracting new insights from complex data. But, as with other forms of AI, they can also increase risks for the business and lead to increased scrutiny by regulators: these tools and technologies could ultimately affect the delivery of critical business services to the surrounding ecosystem.

AI's risks stem from many sources. Among the most important are potential breaches of data-privacy rules in the development of models; a lack of transparency around how these systems work, with the risk that flaws in model design or training-data selection may introduce errors, unfairness, or bias; and new cybersecurity risks such as model extraction or deliberate "data poisoning" by malevolent actors (Exhibit 2).

Most companies do not yet have the appropriate structures and tools to effectively manage the risks and returns of intelligent automation. Specifically, different aspects of system development and operation (such as implementation and system management, risk and resilience management, and business-process optimization) are often managed by various functions in a fragmented way. Furthermore, organizations typically lack robust frameworks, processes, and infrastructure to ensure the effective risk and return assessment of AI and automation. It's therefore increasingly critical for companies to incorporate automation-specific considerations into their broader AI- and digital-risk-management programs.

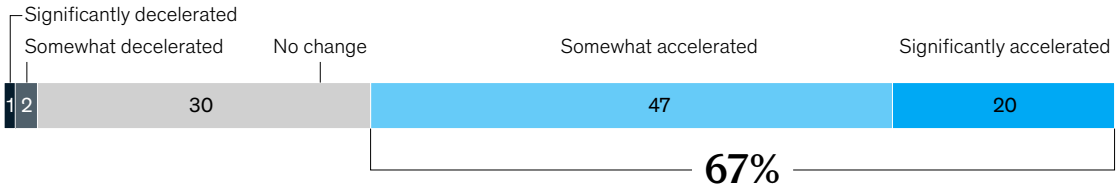
Toward a better understanding of automation risk

To drive strategic decisions across the organization, institutions can create a holistic view of both the benefits and risks of intelligent automation—including where these tools touch critical processes and where there might be vulnerabilities. They also need to understand not only how to simplify and automate processes, but also how to systematically reduce risk and improve institutional resilience. For this purpose, five key tactical steps

Exhibit 1

Companies have accelerated their automation and AI capability building in response to the pandemic.

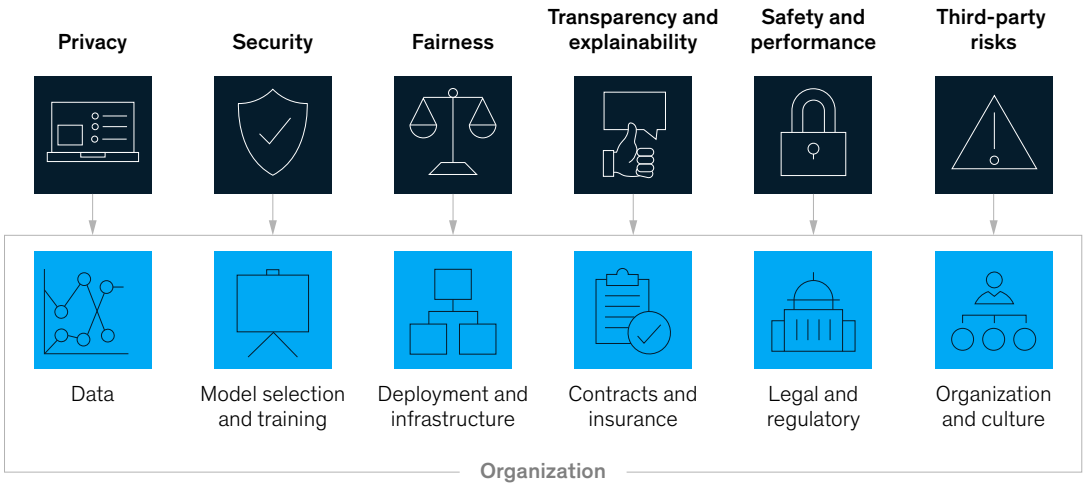
Reported change in adoption of automation and artificial intelligence since the start of the COVID-19 pandemic, % of respondents



Source: McKinsey Global Business Executives Survey, July 2020 (n = 800)

Exhibit 2

AI and automation systems create new risks across an organization.



can be considered across the automation and AI life cycle (Exhibit 3).

Step 1. Establish a dedicated intelligent-automation risk-return center of excellence

The first requirement is to bring all the relevant information and decision oversight together in one place. One way to do this is to establish a dedicated center of excellence (CoE) for intelligent-automation risk-return management. This central function would be responsible for ensuring that AI and automation solutions drive performance and value across business processes, without increasing risk beyond limits defined by the organization.

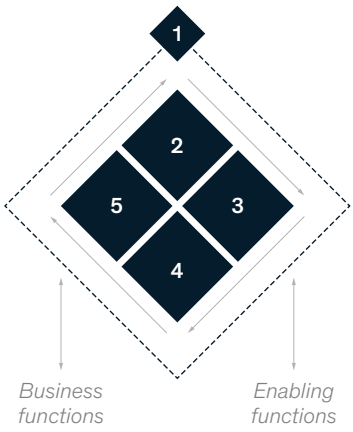
To achieve this objective, the CoE needs a comprehensive view of three things. First, it must understand the enterprise taxonomy of business services and processes across the organization; these become a single source of truth to discuss and navigate the process landscape. Second, it must know where in those processes AI and automation are implemented today, and where there is the potential to increase efficiency or business performance over time through the deployment of additional use cases. Finally, it must have a clear picture of the vulnerabilities identified in current and proposed AI and automation solutions.

Because simple automation solutions typically rely on fairly deterministic approaches, the risks involved are more likely to center on implementation errors or incorrect configuration. That's in contrast to the risks inherent in AI's complex techniques, which are usually designed to tackle uncertainty and thus raise broader sets of potential issues, such as explainability and various forms of bias. Accordingly, automation risks can often be understood as a subset of AI risks.

To build up this picture, the intelligent-automation risk-return CoE can draw on in-house expertise as well as capabilities that exist elsewhere in the business. For instance, in banking, the model-risk-management team would typically provide a view on vulnerabilities identified in AI, such as issues related to bias and fairness in decision making, or to the "explainability" of the underlying models. The CoE would play a strategic role in coordinating activities already performed not only by the model-risk-management function but also by the legal,

Exhibit 3

Five tactical steps can help companies manage the risks and rewards of intelligent automation technologies.



1 **Establish an automation/AI risk-return center of excellence:** ensure that AI and automation solutions drive performance and value across business processes, and within risk limits

2 **Assemble enterprise-wide inventory of opportunities:** identify, compile, and prioritize new and existing AI and automation solutions across all enterprise business functions

3 **Build a standard technology-integration framework:** curate a standardized framework for selection, development, and deployment of potential AI and automation solutions

4 **Assess AI and automation risks:** assess vulnerabilities and risks through comprehensive regimes to test quality, performance, sensitivity, explainability, etc

5 **Design framework for risk monitoring:** develop a robust monitoring dashboard to synthesize AI and automation risks and returns in real time across the enterprise

compliance, and IT teams, extracting relevant information through robust reporting processes.

Step 2: Identify and prioritize opportunities for end-to-end optimization and business simplification

Organizations may already be using a wide range of AI and automation applications, with many more under consideration or in development. The creation and maintenance of a detailed inventory of these applications is a fundamental task for the intelligent-automation risk-return CoE.

This inventory would include information on the methodology and techniques used in each case, as well as the implementation platform, the business processes in question, the owner of the system, and any associated technology vendor. It would also include details about all the potential vulnerabilities identified in the approach. Business units would be required to submit this information to the CoE for each AI and automation application they implement, with regular reviews and audits in place to ensure that information is always up to date. The process could build on existing intelligence: banks' model-risk-management teams typically maintain a model inventory, with a view on AI solutions used across the organization.

The AI and automation inventory supports both sides of the risk-return equation. By providing a complete view of how and where AI is already being used in the organization, the inventory helps leaders identify synergies and opportunities to replicate or expand proven approaches into new areas. At the same time, the inventory enables the CoE to spot risks, identify their owners, and manage any required mitigation steps.

Based on this transversal view of intelligent automation implemented across the organization, the risk-return CoE can make strategic decisions on where to deploy, enhance, retire, or consolidate solutions and technologies. In that context, the organization can establish a framework to prioritize processes based on organizational value and business criticality. For instance, when a global security and cash logistics company with operations across multiple geographies conducted an enterprise-level identification and prioritization effort, leaders were able to define more than 40 strategic existing AI solutions that could be leveraged by other businesses.

Every AI system or automation tool needs to undergo a rigorous and comprehensive test regime to identify any risk of inaccuracy or bias.

Step 3. Develop a robust framework to integrate technology solutions across the end-to-end value chain

In conjunction with relevant analytics and technology teams, the intelligent-automation risk-return CoE can establish a standardized process and set of principles for the development and implementation of AI and automation technologies. The CoE can then work with business units to ensure that these principles are applied consistently across the organization. Doing this increases transparency on organization-wide AI and automation efforts and helps to ensure that key risks and limitations are identified early in the development cycle.

One global bank revisited and rewrote its automation- and AI-development playbook to create a common transformation approach that could be applied across every region and line of business. The playbook's standards reinforced the effective tracking of project risks—including the requirement for specific risk assessments and metrics—together with the transformation's impact, returns, and additional benefits. Equally important, a rigorous prioritization system encouraged a focus on the most critical applications, processes, and services. This framework helped the bank understand—for the first time—the limitations of the AI and analytics systems used across the organization, allowing it to define robust mitigating controls.

Step 4: Assess AI and automation risks

Every AI system or automation tool needs to undergo a rigorous and comprehensive test regime to identify any risk of inaccuracy or bias in the input, processing components, and output. At minimum, the assessment would typically encompass data quality (such as the risk of error or bias in the data sample), correctness of implementation (including the deployment of the correct formulas and rules), the performance, sensitivity, and robustness of the system (focusing on output accuracy), the explainability of the model (given its use cases and complexity), and any bias and unfairness in the results it generates. Some types of tests, including those for security weaknesses or susceptibility to data poisoning, may require the services of specialist in-house or third-party teams.

In industries such as banking, functions overseeing analytics risk assessment (such as model-risk management), together with the analysis they perform, can support decision making on AI applications. One large US bank had developed several AI and automation solutions as part of its digitization journey, including chatbots, optical character recognition (OCR) technology, robotic-process automation, and speech-to-text techniques. An independent review and challenge process, conducted as part of the bank's standard oversight practices, identified a series of opportunities to mitigate risks and increase the efficiency benefits generated by these systems.

For example, instability issues arose regarding the OCR techniques. Too often, the method chosen misconstrued characters in customer-account identifiers—the letter "O" interpreted as the

number “0,” or the number “5” interpreted as an “S.” These inaccuracies would incorrectly map customer information in relevant systems and require multiple human interventions to correct the errors manually. Controls were implemented to ensure that cases at risk were identified and processed at an early stage in a controlled way without affecting customers.

Elsewhere, chatbots were planned for production without a robust monitoring plan to ensure that future changes (such as adding new languages or functions, including access to sensitive banking information) were identified and controlled before deployment. Introducing such a plan protected the bank from potential financial or reputational risks. It also allowed the institution to track increases in efficiency, such as by measuring decreased need for human intervention in basic customer interactions.

Step 5. Design a framework and infrastructure to monitor risk and returns

Finally, since decisions need to be made on an ongoing basis, companies can define processes to monitor benefits and risks of AI and automation over time. In that context, a robust monitoring framework and infrastructure needs to be built, with well-defined performance and risk indicators. Such frameworks are already used in the banking sector, although their focus has hitherto been limited to risk. Creating a perspective that combines both the risks and benefits of AI and automation technologies is a critical step to drive strategic business decisions across the organization.

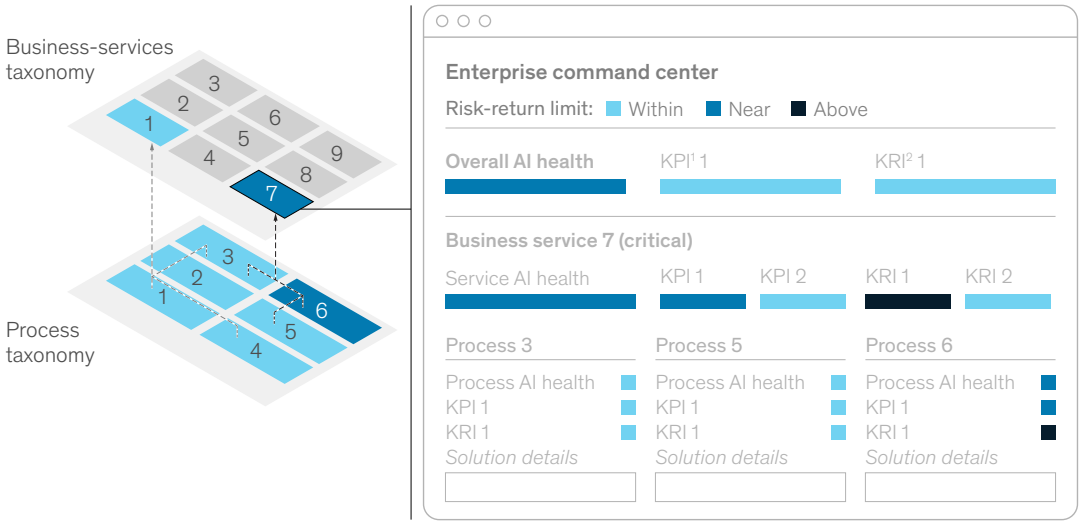
The monitoring would ideally provide a dashboard with an aggregate view of automation and AI across the organization, together with solution-specific information where required (such as the last time the AI was tested, the level of benefit observed over time, and any performance deterioration). Eventually, this would allow the creation of a real-time heat map and dashboard for action by the intelligent-automation risk-return CoE (Exhibit 4).

This monitoring would be accompanied by an issue-management procedure for effective remediation

Exhibit 4

A real-time dashboard monitors AI risks and returns, revealing which processes are sources of risk.

Illustrative AI risk dashboard



[1]Key performance indicator.
[2]Key risk indicator.

of errors and limitations identified in AI tools and automation systems. It would also escalate cases in which efficiency is deteriorating over time, and a system needs to be enhanced or redeveloped.

Intelligent automation is already transforming the efficiency and effectiveness of many business processes. As companies seek to expand their use of these technologies through wider application and the adoption of more sophisticated approaches, however, they are also exposing themselves to ever-greater risks. Balancing these risks against the potential returns of automation and AI will be a critical challenge in the coming years. Organizations that put the right structures, systems, and governance measures in place today will be able to unlock significant improvement potential.

Federico Berruti is a partner in McKinsey's Toronto office, where **Akshay Phal** is a specialist; **Christophe Rougeaux** is an associate partner in the Boston office.

Designed by McKinsey Global Publishing