It may sound like a sci-fi plot but it’s true, the bots are here, they are significantly impacting our jobs and in extreme cases, replacing them entirely. Robotic process automation (RPA/RBPA) technologies are invading nearly every aspect of business operations, enabling the automation of everything from customer interactions to order processing, equipment maintenance to product packaging, and data collection to market analytics.

There is plenty to be gained from embracing our new digital co-workers. With the ability to interpret incoming data and take appropriate actions without manual intervention, bots can optimize the cost and speed of overall business operations. They can also be configured to pull market insights from large data sets, reduce human errors in data entry processes, assist in audit and compliance activities, and dramatically reshape the customer experience.

Assuming, that is, they work as expected.

No doubt, the proliferation of RPA technologies is occurring at far greater speeds than many can control. And without the proper controls, even the smallest miscalculation or unchecked vulnerability can bring a company to its virtual knees. So the bots are here, but how do we control them?

Understanding the bot-risk

It is true RPA technologies have the potential to re-shape industries, but they are not magic bullets. Without proper governance and risk control strategies, all it takes is one malfunctioning bot to disrupt a system with bad information or perform erroneous actions with long-term consequences. Moreover, without the proper security checks and underlying controls, it’s not impossible for bots to be exploited by outside agents to steal sensitive data or conduct larger-scale sabotage.

Not that these risks should dissuade organizations from adopting automation. Indeed, with the right approach, the new wave of robotic automation has the potential to transform organizations for the better, giving them untold advantages over the competition. Yet like any other transformation, embracing robotic automation demands a well-designed risk and governance strategy to help ensure any and all risks associated with the digital transformation are identified, evaluated, and dealt with for good.

Strategizing bot-risk control

Technology, process, people. These are the pillars of the intelligent automation ecosystem. Each play an integral role in the successful implementation of RPA technologies and, as such, each must be considered when designing a risk governance framework.

As for the shape of that framework, a successful and sustainable approach to managing the risks of bot integration will include plans across three core areas:

- **Strategy:** Organization’s risk and governance functions should play a key role in defining the governing strategy and evaluating the automation platform and a pipeline of automation use cases. For example, defining a risk profile and tolerance based on the organizational, functional, industry and regulatory landscape and compliance requirements.

- **Delivery:** The risk and governance function should support a process of secure and scalable bot development, quality assurance and controls integration. In part, that means embedding risk management in the delivery of solutions through the deployment of training, toolkits, and templates. This will help identify, evaluate and mitigate risk associated with initial development and delivery of bots and the ultimate expansion of the intelligent automation program.
Operations: The risk and governance function should enable effective program monitoring, including key risk and performance indicators and value-driven data analytics. For example, one should establish key risk indicators (KRIs) throughout the ongoing operation of the program.

Bringing bots to life: Plan, build, deploy and run

It’s easy to talk about integrating risk and governance throughout the automation journey. The hard part is taking action. Fortunately, there are many tangible actions an organization’s risk and governance function can take when strategizing, delivering and operating bots to keep the intelligent automation program under control. These can be distilled into three core phases, or activities, that make up your intelligent automation implementation program: plan, build, and run.

Plan

What are you designing your bot to do? Automate a process? Increase speed to market? Reduce overhead or redundant costs? Understanding the nature, impact, and complexity of your automation program use is one of the first steps towards identifying and managing the potential risks. The second is ensuring the technology platforms align with the company’s vision and can scale alongside it.

Once you define your risk appetite, requirements, and scope, the next move is to design a risk and governance framework that includes plans about who will ‘manage’ the implementation of the bot and who will be responsible from that point forward to ensure it is working as expected. After all, they may not take lunch breaks or call in sick, but bots should still be treated as employees.

Build

It’s not enough to simply perform an initial risk review of your intelligent automation platform. Risk management strategy needs to be embedded from the beginning, implemented in the build stage, and monitored on an ongoing basis. And remember, risks can change as your solution scales. As the technology evolves and enhances, so may your risk exposure.

At the build stage, your risk and governance function is responsible for overseeing the intelligent automation program. The function should perform initial due diligence and risk reviews of automation solutions, design and implement platform controls, and play an active role in 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.

Run

Supporting one’s intelligent automation program from a risk and governance perspective 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 KRIs and key performance indicators (KPIs) associated with the automation program and report them to key stakeholders in order to help optimize and scale the program using relevant data and analytics. Moreover, the function should establish business continuity and disaster recovery plans in the event of automation downtime and failures, and 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.

Worth the risk

There are a great number of efficiencies and benefits to be gained from automation. Given the promise of faster processes, lower labour costs, and more accurate outcomes, it’s clear that RPA technologies are among an organization’s first choice for staying ahead of the competition.

Still, starting on the often daunting journey of an important digital transformation project demands great attention to the risks involved. That’s where a well-considered risk and governance plan, created with support from experienced technology risk consultants and experts, can help organizations lead the charge and control bot invasion.

Contact:
Pushkar Sharma
Technology Risk Consulting
KPMG in Canada
prsharma@kpmg.ca

kpmg.ca/rethinkrisk
#rethinkrisk