Risk and control considerations within robotic process automation implementations

Balancing transformation with risk and control to achieve compliance

EY
Building a better working world

Addressing history before it repeats itself

Since the advent of technology as a vehicle to accelerate business performance within organizations, risk management has often been perceived as a foundational, yet sometimes burdensome, pillar that has frequently been sidestepped since inception. For example, during the early 1980s, spreadsheets and databases (collectively, referred to as end-user computing (EUC)) began to multiply at an astonishing pace due to their ease of use, functionality and powerful insights that could be gleaned at record speed. However, even today, this domain remains a considerable impediment for organizations because sustainable, control-focused programs were not established from the onset to govern, assess, standardize, and monitor performance and risk. Retroactively untangling the unwieldy universe of EUC is often viewed as a Herculean (and, potentially, even insurmountable) task within organizations and unfortunate headline-worthy instances have resulted, including:

- **Human error**
  - After releasing earnings, a multinational home mortgage funding company **restated** its **unrealized gains by $1.2 billion** due to "honest mistakes made in a spreadsheet used in the implementation of a new accounting standard."
    Source: Gartner
- **Fraud**
  - A global investment bank identified a macro with **intentionally inappropriate linkages** utilized to create **fictitious transactions** and depict inaccurate growth.
    Source: Forrester
- **Data privacy**
  - **Forty-six percent of data privacy incidents** are a result of compromised files by internal resources due to uncontrolled access to data files residing on shared drives.
    Source: CIO World

Organizations possess the luxury of hindsight to reflect on future improvements. EUC is a comparable example whereby an investment to harness risk and control up front may have minimized a perennial dilemma across the financial services industry. It is imperative for organizations to address the risks presented and consider the potential implications introduced relative to the vision, reputation and success of an organization (e.g., inaccurate financial reporting, operational losses and inefficiencies, fraud, reputational risk, consumer concern, regulatory sanctions and strategy growth limitations).

What will be the catalyst for organizations to harness the risks introduced by RPA to mitigate a similar dilemma within the next decade?

State of robotics

More recently, the financial services industry has embraced automation as a disruptive force that challenges the current state of daily business operations, while simultaneously aligning with organizational drivers (e.g., cost, productivity and efficiency). Although the continuum of automation ranges from basic workflow through artificial intelligence (inclusive of machine learning, natural language processing and cognitive processing), organizations have begun to invest heavily in robotic process automation (RPA). This technology allows organizations to automate high-volume, deterministic, system-based tasks by introducing a virtual workforce of **"robots."** The business units that comprise the first line of defense (specifically, the finance and operations departments) have been the earliest adopters of this advancement. They evaluated their existing processes to identify, prioritize, develop and, ultimately, deploy robotics that may alleviate mundane tasks and departmental pain points. Business units have capitalized on the speed and nimbleness of deploying RPA in partnership with and, at times, autonomously from IT departments.

28% of firms have automation-deployed technology today.*

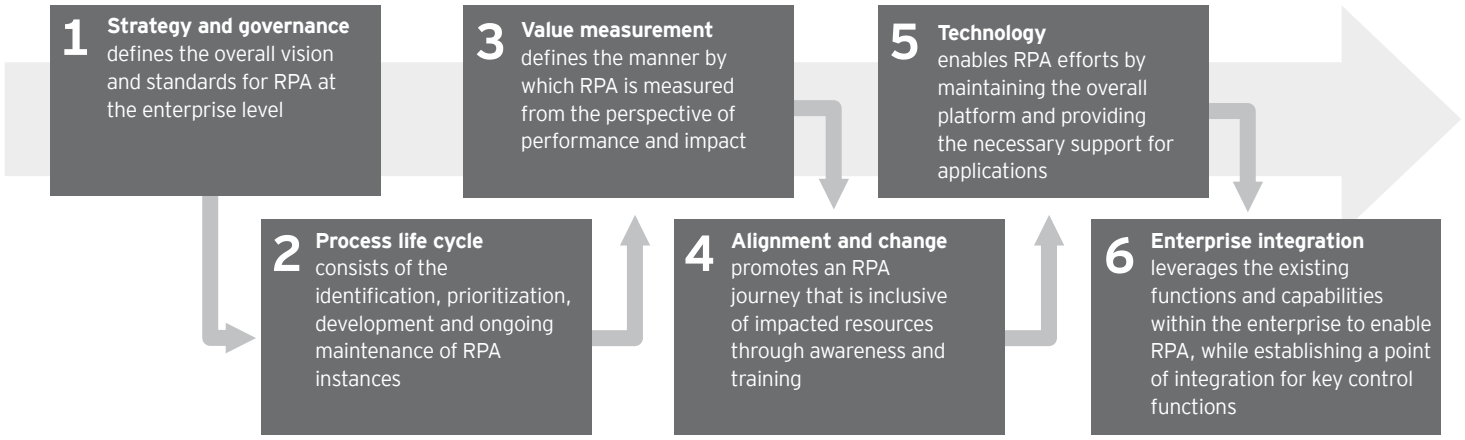
40% of management teams think automation is the most enabling enterprise technology.*

50% of global IT service centers are actively pursuing automation pilots.*

$4.9b is the estimated size of the global automation market by 2020.*

* "RPA is Transforming Business Process – Delivering Fast, Accurate Service, and Improving Customer Experience," Everest Group, Institute for Robotic Process Automation, 2016.

As the appetite, quantity and complexity of robots begin to proliferate following adoption across the three lines of defense, organizations recognize the necessity to establish program governance from the onset to enforce consistency, accountability and standardization. The creation of a scalable operating model is a vital undertaking to balance strategy formalization, business enablement, technology integration, and communication and coordination. The decision whether to embrace a federated or centralized operating model construct is a function of an organization's culture, but most traditional RPA operating models consist of the following six components.

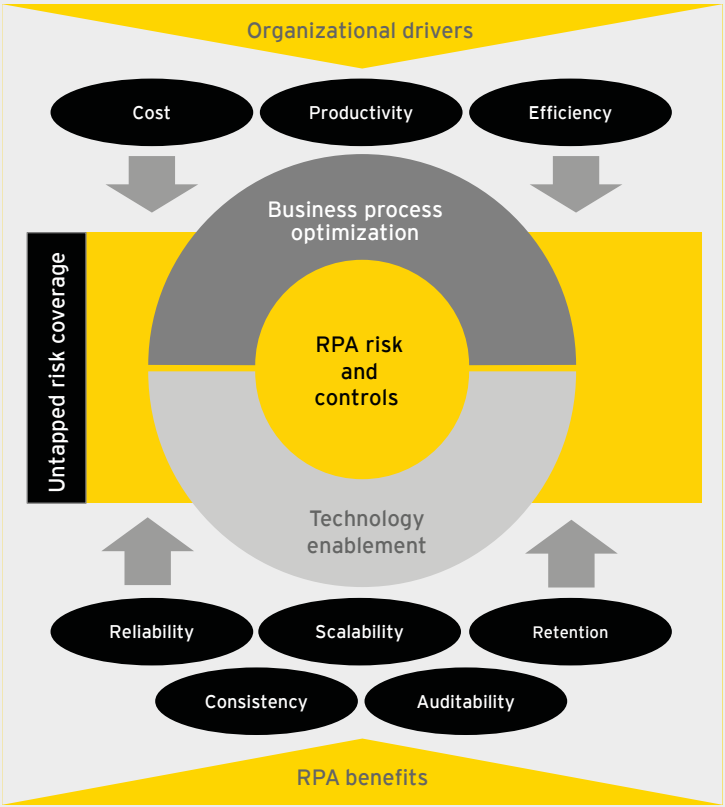


Organizations are also instituting formal centers of excellence (COEs) that align with this broader operating model. These COEs represent dedicated groups with specialized competencies that focus on orchestrating the RPA life cycle. These organizational structures (e.g., operating models and COEs) remain governance focused, yet their primary business objectives are optimizing the connectivity of disparate processes to build **"bridge"** functionalities, creating efficiencies and improving productivity. As the continuum of automation progresses beyond RPA, organizations ultimately should reflect upon the lessons learned from their RPA journey to proactively institute similar COE constructs and recognize risk and control considerations.

Although RPA may enhance the overall interconnectedness of business process operations, how is the risk and control landscape impacted by the introduction of such transformational automation initiatives?

Recognition of risks and controls

As the financial services industry entertains this inflection point of puzzlement, curiosity and concern surrounding RPA across organizations, the question is no longer **"if,"** but rather **"why," "when," "how many," "where"** and **"how fast"** robotics have been deployed. Boards, executives, committees, regulators, risk management and compliance functions, and internal audit departments are receptive to leveraging technology to reduce costs and streamline processes, yet queries have arisen about the parallel degree of focus on risk, control and compliance. Instances have also been identified whereby control consciousness has been viewed as secondary to deploying RPA and realizing business returns.

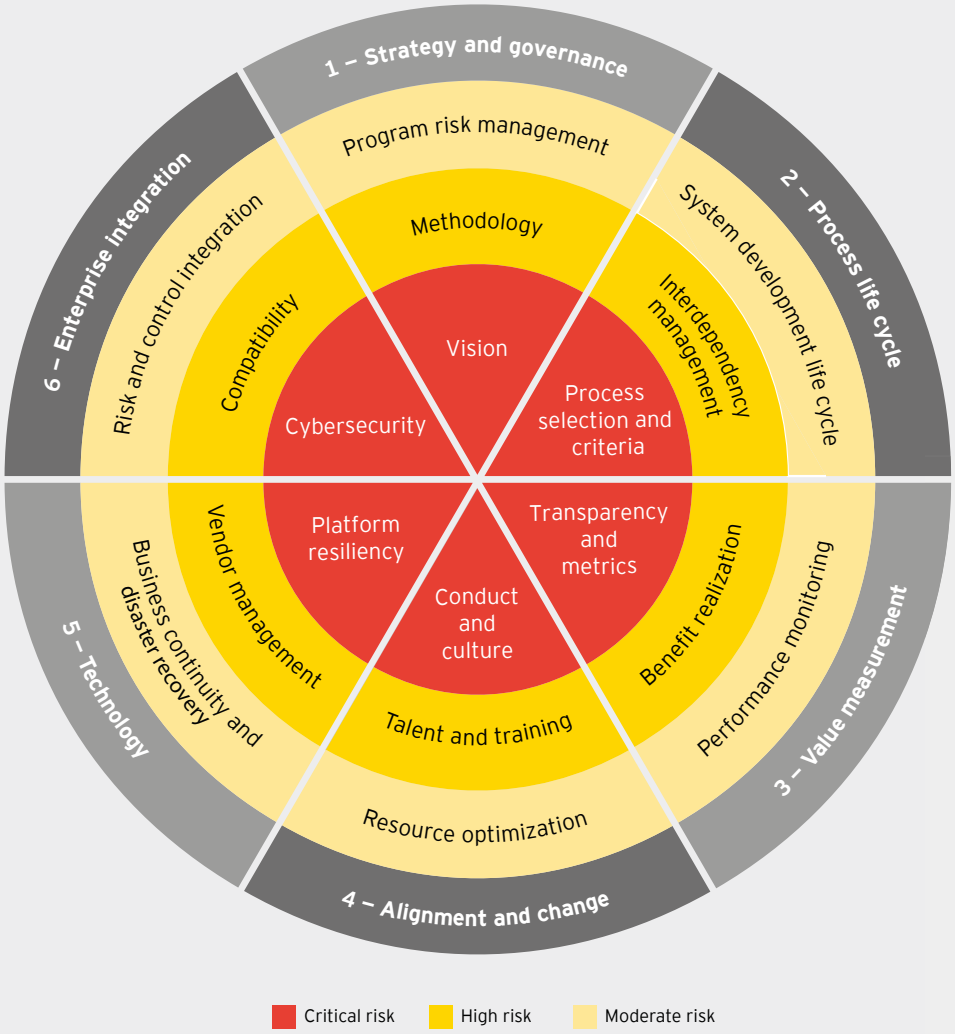


Risk mitigation remains the foundation for strong business performance, and organizational trepidation has surfaced that robotic deployments may be a new vehicle that presents both traditional risks and also introduces new, unforeseen risks. Minimally, from a risk and control perspective, organizations are tackling the following representative apprehensions with their RPA journey.

- **Rationalization** – Although organizational direction may be communicated with regard to RPA, anxieties exist regarding the improper usage and deployment of robotics. RPA sometimes may rightly serve in a bridge capacity, but situations have occurred whereby RPA is not the appropriate technology and was solely selected due to a speed-to-market goal. As a result, the advantages of flexibility and convenience have been a curse, and led to knowingly circumventing extensive queues within development teams and cumbersome technology controls.
- **Maintenance and operations** – Similar to an employee, robots require guidance to perform the activities desired. Although robots are configured as of a point in time based upon defined business requirements, broader architecture and system changes can severely affect the expected performance. Modified data field mappings, orphan and dangling robots, vendor upgrades, system integrations, capacity and performance monitoring, and forward compatibility considerations require attention to preserve the original intentions of the robot and manage the perceived brittleness of the application and RPA dependencies.
- **Cybersecurity and resiliency** – As robotics become mainstream, these new entrants to the IT environment represent additional vectors for compromise. Abuse of privileged access, mismanaged access entitlements and disclosure of sensitive data are valid concerns. Additionally, platform security vulnerabilities, privacy implications and denial of service may yield ramifications that impact the RPA integrity, reliability and downstream business processes.
- **Methodology and documentation** – Granted that agile development methodologies encourage improved iterative communication and coordination between key stakeholders, adherence to documentation standards should be a staple of this approach to support the risk and control mindset. Although business functionalities may be delivered more timely and accurately, the traceability of artifacts related to RPA decisions often is absent, and even an afterthought.

Regardless of an employee's role within an organization, it is widely appreciated that regulatory, financial and reputational risk management are simply **"good business."** Automation agendas are exciting and groundbreaking, yet they require an effective challenge from a risk management perspective to proactively protect organizations. As robots extract, aggregate, transform and upload data, risk and control considerations become paramount discussion topics.

Illustrative risks per operating model component



Why are my actions related to data (e.g., extracting, aggregating and transforming) suddenly under extensive scrutiny?

Proactive risk and control consciousness

To complement the prior RPA organizational structures (e.g., operating models and COEs) discussed, it is critical to identify the junctures of risk introduced by the broader RPA program. The following represent illustrative risk considerations in which a degree of control may be justified.

1. Strategy and governance

- ☐ Has an organization-wide, business-driven vision and strategy been defined, inclusive of the end state and maturity tollgates (e.g., operational readiness, benefit realization and virtual workforce)?
- ☐ Has an operating model (inclusive of program roles and responsibilities) been established to govern, manage, operationalize and scale the program and life cycle (e.g., centralized and federated)?
- ☐ Have policies and standards been defined to promote program value and consistency (e.g., process prioritization, value measurement, development and deployment, issue management, and risks and controls)?
- ☐ Has a project management office been established to foster a "seat-at-the-table" position across relevant steering committees to focus on RPA development workflow, financial planning, resource management, and control and risk management aspects?

2. Process life cycle

- ☐ Has a consistent, end-to-end methodology been established to manage the RPA life cycle (e.g., identification, prioritization and development)?
- ☐ Have process suitability criteria been established (e.g., deterministic, digitized and documented) and are potential candidates stored within a repository for future consideration?
- ☐ Has a process prioritization model been defined to align with the business-driven program vision and the desired value (e.g., efficiency gains, cost avoidance, quality management and growth acceleration)?
- ☐ Has exception handling of the processes in production been conducted to monitor performance (e.g., run-book protocols) and manage any encountered exceptions (e.g., technical or operational)?

3. Value measurement

- ☐ Has a regular cadence been established to communicate the program's progress and success to executive leadership (including progress relative to the overall strategy, vision and maturity)?
- ☐ Have key performance indicators (KPIs) and key risk indicators (KRIs) been defined to proactively assess the RPA program's health (e.g., engagement and acceptance, efficiencies gained, development pipeline and training)?
- ☐ Have operational and performance metrics been defined to identify trends and anomalies regarding production concerns (e.g., capacity, downtime and exceptions)?
- ☐ Has the return on investment been measured (e.g., cycle time, transactions processed and capacity gains) and socialized to challenge the speed and targets for further automation?

4. Alignment and change

- ☐ Has the organization planned accordingly for the new competencies required to sustain the RPA program strategy?
- ☐ Has organizational training and education been deployed (and how frequently) to provide the necessary skills uplift (e.g., awareness, foundations and development)?
- ☐ Have new learning paths, job descriptions and workforce planning changes been defined to promote the program's sustainability?
- ☐ Have automation anxiety and resistance and cultural impacts been experienced organizationally?

5. Technology

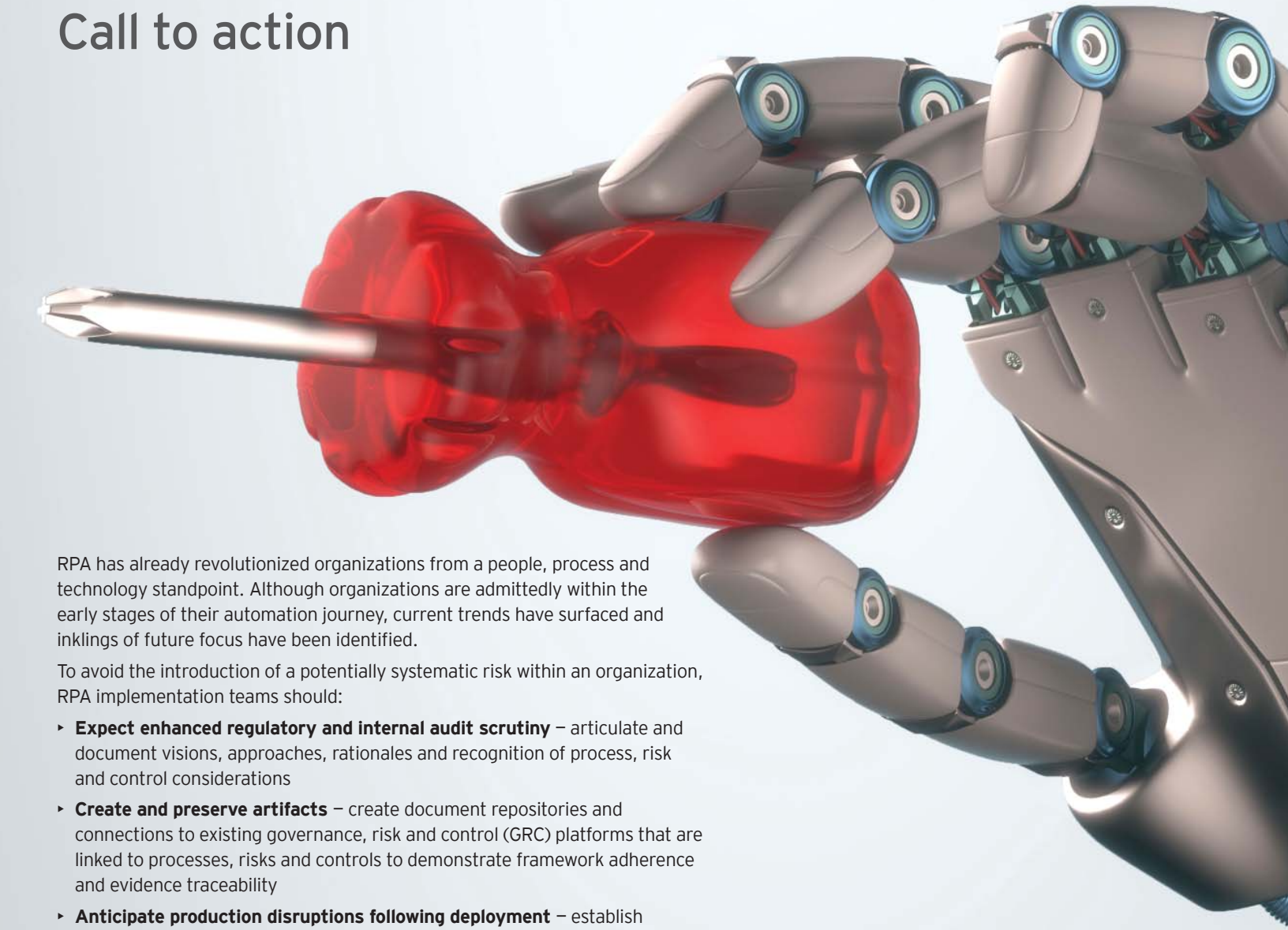
- ☐ Has the organization effectively collaborated with the RPA vendor to agree upon licensing, communication channels, interaction points and service-level agreements (e.g., software issues, configuration management, enhancements and defects)?
- ☐ Has the organization challenged the compatibility of RPA with the underlying architecture and infrastructure (e.g., synchronization, server changes, entitlement management, business continuity and disaster recovery)?
- ☐ Has a controlled, non-production innovation and test lab been established to challenge the feasibility of the integration of RPA with further emerging technologies?
- ☐ Has a knowledge-management repository been established to capture relevant RPA lessons learned, accelerators, enablers and artifacts to promote organizational consistency?

6. Enterprise integration

- ☐ Have RPA teams effectively integrated with organizational transformation teams to maximize synergies (e.g., business process management) and minimize duplication?
- ☐ Have the three lines of defense adopted standardized risk and control frameworks that align with the RPA operating model?
- ☐ Have the security implications (e.g., privileged access management, denial of service and platform vulnerabilities) and regulatory implications (e.g., privacy and across borders) of RPA been proactively considered?
- ☐ Has the impact on core technology processes (e.g., change management and logical security) and system integration been evaluated and communicated as a result of introducing RPA?

How has your organization demonstrated the agility to tackle the risk and control agenda for these domains to provide enhanced visibility of the RPA program's soundness?

Call to action



RPA has already revolutionized organizations from a people, process and technology standpoint. Although organizations are admittedly within the early stages of their automation journey, current trends have surfaced and inklings of future focus have been identified.

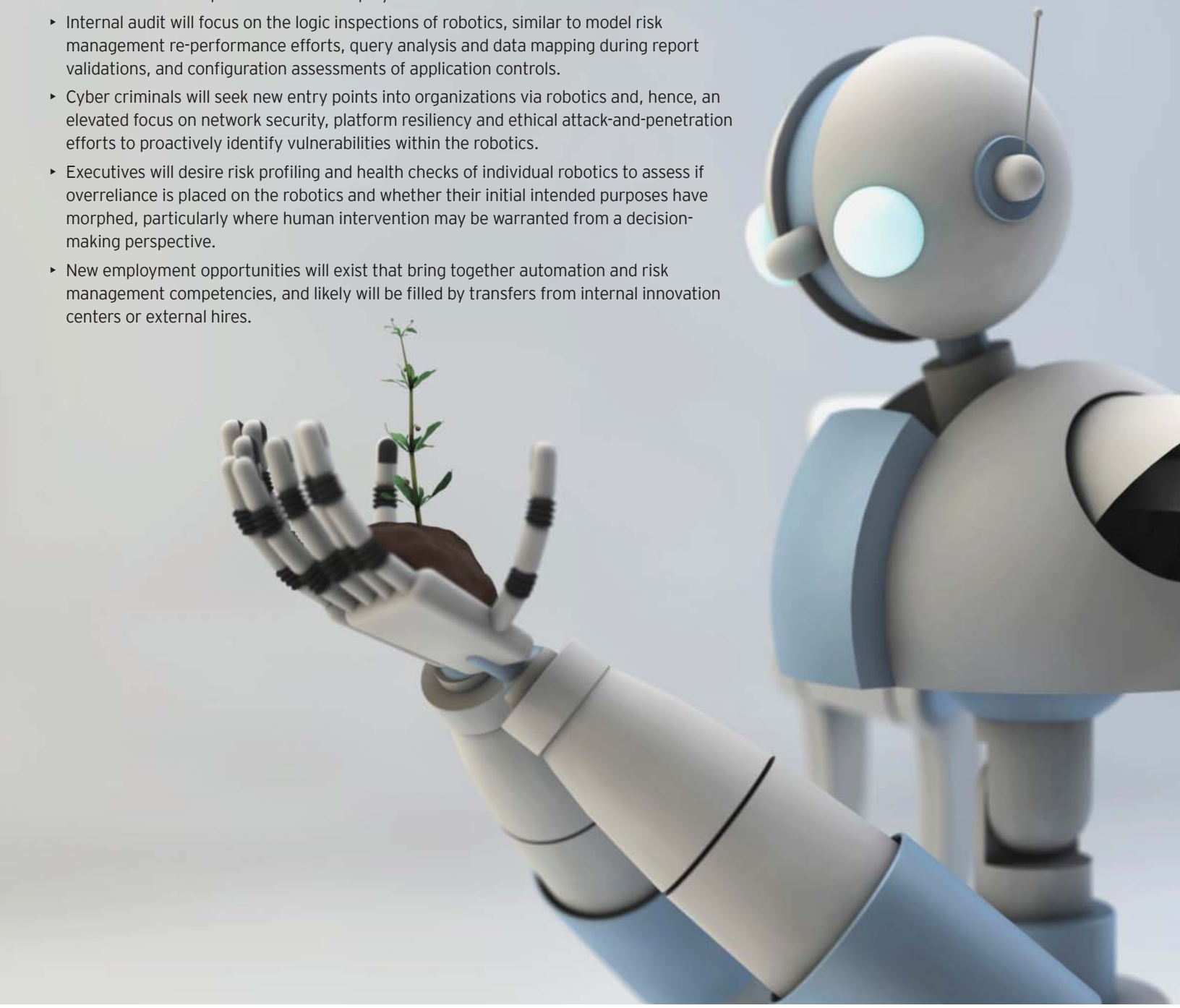
To avoid the introduction of a potentially systematic risk within an organization, RPA implementation teams should:

- **Expect enhanced regulatory and internal audit scrutiny** – articulate and document visions, approaches, rationales and recognition of process, risk and control considerations
- **Create and preserve artifacts** – create document repositories and connections to existing governance, risk and control (GRC) platforms that are linked to processes, risks and controls to demonstrate framework adherence and evidence traceability
- **Anticipate production disruptions following deployment** – establish handling procedures for timely resolution of issues identified to minimize the impacts on connected operations
- **Embed risk and control involvement** – entertain the inclusion of a dedicated work stream to proactively foster risk and control consciousness, including participation in a **seat-at-the-table** capacity during agile development working sessions (e.g., Scrum)
- **Assess consistency of control process, risk and control inventories** – determine overlaps and disparities with the organization's technology risk and control inventory
- **Plan accordingly for delayed deployments** – recognize that stage gates (and, therefore, buffers) may need to be incorporated into timelines to manage risk and control implications during agile development efforts
- **Challenge the audience and degree of progress and risk reporting** – understand the desire for reporting about benefit realization, concentration risk, control adherence and resulting people risk management
- **Consider synergies of the risk and control work stream** – recognize that content within a process, risk and control work stream can be pivoted to serve as an internal audit work plan to evaluate the RPA implementation
- **Determine the new role of people** – recognize that roles and responsibilities will be altered as a result of RPA implementations, yet oversight and monitoring are critical to foster control and sustainability

Top-five predictions

The emphasis on cohesive processes, risks and controls remains a staple across the financial services industry. Although new disruptive innovations and technologies will be introduced into an organization's environment as time elapses, we believe:

- Regulators will take considerable interest with regard to the handling of people risk management, particularly since robotics may alienate or create angst among employees and their future responsibilities and employment.
- Internal audit will focus on the logic inspections of robotics, similar to model risk management re-performance efforts, query analysis and data mapping during report validations, and configuration assessments of application controls.
- Cyber criminals will seek new entry points into organizations via robotics and, hence, an elevated focus on network security, platform resiliency and ethical attack-and-penetration efforts to proactively identify vulnerabilities within the robotics.
- Executives will desire risk profiling and health checks of individual robotics to assess if overreliance is placed on the robotics and whether their initial intended purposes have morphed, particularly where human intervention may be warranted from a decision-making perspective.
- New employment opportunities will exist that bring together automation and risk management competencies, and likely will be filled by transfers from internal innovation centers or external hires.



Next steps

To provide constructive, timely feedback and challenge regarding the risk and control considerations of an RPA implementation, it is critical to strike a balance between passive and obtrusive engagement. The majority of implementations today do not possess a dedicated risk and control work stream as part of the broader project team. The integration of this focused risk and control mindset throughout the process would serve as a dynamic preparedness health check in advance of the inevitable external review and overall stakeholder inquisitiveness.

As echoed earlier, risk and control compliance should not be sacrificed during the automation journey. These disciplines are not mutually exclusive, but rather they should coexist in harmony. As organizations continue to progress their automation agendas, the following actions should be considered:

- Assess feasibility of a **"bolt-in"** risk and control work stream for robotic implementations underway to retrofit artifacts, where possible
- Understand future robotic implementations to consciously align a **bolt-in** risk and control work stream from the start
- Evaluate degree of preparedness documentation required for external-party review (e.g., rationalization, robotic playbooks, robot inventories, flowcharts, and risk and control matrices)
- Develop templates and enablers to capture relevant risk and control documentation on an ongoing basis, including performance of a risk-based degree of design and operating effectiveness testing
- Determine necessary skills uplift (e.g., training and development) or hiring required to support risk and control work streams

Maintaining a "finger on the pulse" of RPA risk and control across an organization represents a worthwhile *investment* to proactively manage the changing business processes and, ultimately, protect against potentially newsworthy repercussions.

Measure and monitor your RPA risk and control profile before becoming a statistic.

Contacts

David Kahan
Financial Services
Technology Risks and Controls
david.kahan@ey.com

Andrew Oltmanns
Financial Services
Business Risks and Controls
andrew.oltmanns@ey.com

George Kaczmarskyj
Financial Services
Robotic Process Automation (Americas)
george.kaczmarskyj@ey.com

Chris Lamberton
Financial Services
Robotic Process Automation
(Europe, Middle East, India, Africa)
clamberton@uk.ey.com

Andy Gillard
Financial Services
Robotic Process Automation (Asia-Pacific)
andy.gillard@au.ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. 00422-181Gbl
1712-2504420

ED 1/18