Deloitte.

Auditing the risks of disruptive technologies
Internal Audit in the age of digitalization

The age of digitalization

We're in the midst of an exciting convergence. Technological advances and trends in advanced analytics, robotic process automation (RPA), and cognitive intelligence (CI) are rapidly reshaping business models, improving productivity, and enabling innovation in the way organizations connect products and services to their consumers. The widespread adoption of these advances is now generally being referred to as Industry 4.0 or the Fourth Industrial Revolution (see figure 1).

This makes for an intricate coordination. As companies continue to adopt emerging technologies, Internal Audit (IA) must proactively assess and gain insight into the new risks associated with these technologies. Doing so will enable IA to assess whether appropriate controls are being implemented to prevent and detect new and emerging risks.

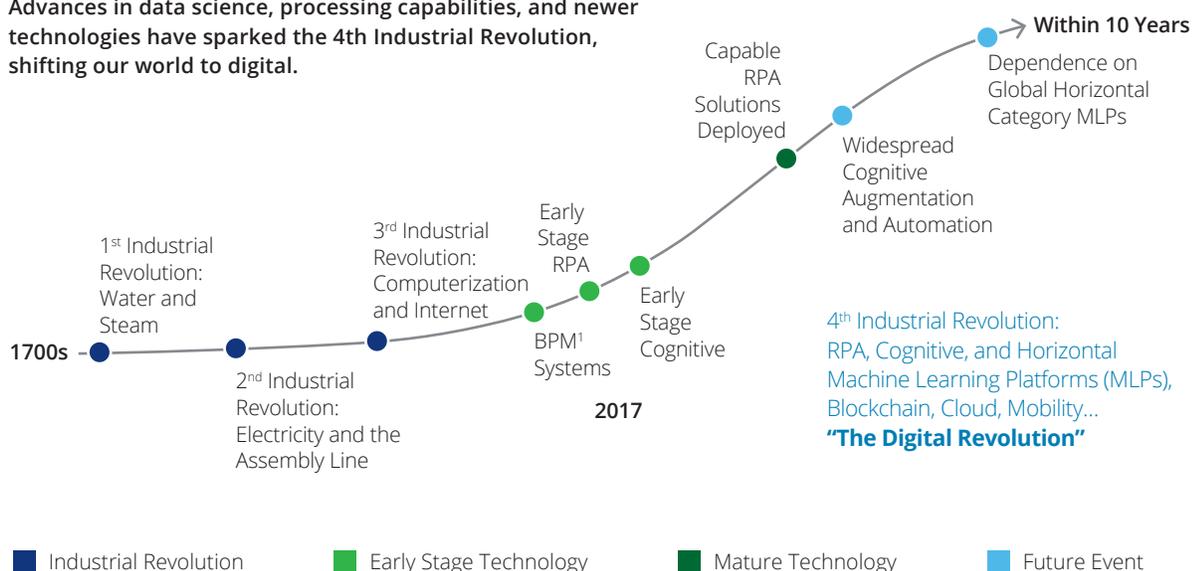Many IA departments have made advancements in addressing these disruptions. While some may be more mature with their approach than others, most departments are in the early phases of the journey. In addition, they want to leverage advanced technologies to further modernize and enhance the effectiveness of their programs, thus creating a need to manage the associated risks.

Currently, a host of technologies are rapidly advancing Industry 4.0, including more interconnected and powerful networks, high-performance computing, and the advent of digital tools, including data analytics, RPA, and CI. Combined, these technologies are changing business in profound ways.

The focus of this paper is on digitalization. In the following pages, we'll take a closer look at the specific risks associated with disruptive digital technologies and offer suggestions to help IA departments assess these risks.

Figure 1. Industry 4.0

Advances in data science, processing capabilities, and newer technologies have sparked the 4th Industrial Revolution, shifting our world to digital.

1st Industrial Revolution: Water and Steam

1700s

2nd Industrial Revolution: Electricity and the Assembly Line

3rd Industrial Revolution: Computerization and Internet

BPM[1] Systems

Early Stage RPA

Early Stage Cognitive

2017

Capable RPA Solutions Deployed

Widespread Cognitive Augmentation and Automation

Within 10 Years

Dependence on Global Horizontal Category MLPs

4th Industrial Revolution: RPA, Cognitive, and Horizontal Machine Learning Platforms (MLPs), Blockchain, Cloud, Mobility… **"The Digital Revolution"**

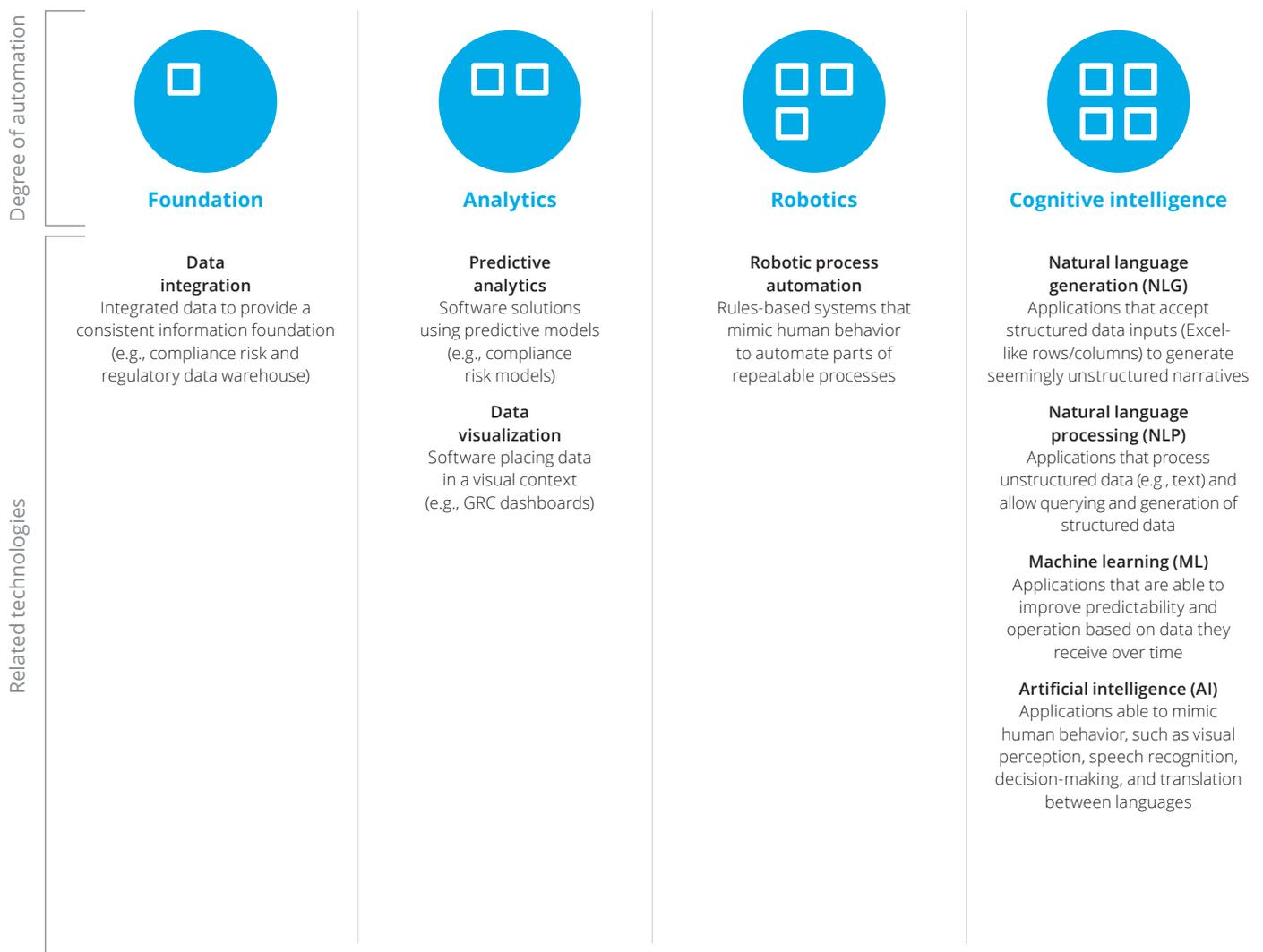■ Industrial Revolution   ■ Early Stage Technology   ■ Mature Technology   ■ Future Event

Source: Industry 4.0: Challenges and Solutions for the Digital Transformation of Exponential Technologies, Deloitte AG, 2015 and Deloitte proprietary research.

[1]   Business process management

Disruptive digitalization

Disruptive digital technologies build upon—and extend— foundational and analytical technologies. By introducing new automation capabilities through RPA and CI, disruptive digital technologies can offer IA large gains in efficiency and effectiveness. Many leading companies have adopted one or all of the technologies shown in figure 2 to manage their day-to-day operations. Therefore, IA departments at these organizations must stay in step.

Figure 2. The digitization spectrum

Degree of automation

Related technologies

Foundation

Data integration
Integrated data to provide a consistent information foundation (e.g., compliance risk and regulatory data warehouse)

Analytics

Predictive analytics
Software solutions using predictive models (e.g., compliance risk models)

Data visualization
Software placing data in a visual context (e.g., GRC dashboards)

Robotics

Robotic process automation
Rules-based systems that mimic human behavior to automate parts of repeatable processes

Cognitive intelligence

Natural language generation (NLG)
Applications that accept structured data inputs (Excel-like rows/columns) to generate seemingly unstructured narratives

Natural language processing (NLP)
Applications that process unstructured data (e.g., text) and allow querying and generation of structured data

Machine learning (ML)
Applications that are able to improve predictability and operation based on data they receive over time

Artificial intelligence (AI)
Applications able to mimic human behavior, such as visual perception, speech recognition, decision-making, and translation between languages

Overview of IA—past, present, and future

Where it all started: Data integration

Companies must be able to analyze data quickly and consistently in order to drive improvements across the enterprise in real time. This requirement has created a strong environment for innovative growth, with data integration as the underpinning of successful automation.

What has recently been done: Analytics

Companies are increasingly harnessing analytics to illuminate patterns, insights, and opportunities hidden within their ever-growing data stores. The exploration can take place to understand future trends and risks by using predictive analytics. Organizations can also deploy data visualization for meaningful and comprehensive visual context.

Where we are now: Automation

RPA is the use of software to perform rule-based tasks in a virtual environment by mimicking user action on the interface, often working on multiple systems. Companies are showing significant interest in adopting RPA, as the automation of time-consuming activities can lead to greater efficiency, allowing staff to focus on more rewarding and higher value activities. Another benefit is scalability, which can improve response to peaks and valleys in demand and volume.

What's next: CI

Advanced CI technologies, such as natural language processing and machine learning, employ algorithms to:

• Extract concepts and relationships from data

• "Understand" their meaning

• Learn from data patterns and prior experience, extending what humans and machines could do on their own

As companies adopt automation initiatives, they introduce new technologies into the enterprise environment. These new technologies, in turn, present new risks to the existing control environment. If not managed appropriately across the three lines of defense, these risks can erode or eliminate value.

For the remainder of this report, we are going to focus on the specific risks of RPA and CI. IA departments should encourage the stakeholders involved to assess the risk of implementing smart automation technologies. This assessment can begin with the following questions:

How will you ensure that these bots* adhere to policies?

Is there an incident management framework to keep bots in check?

How will you prevent bots from proliferating errors?

How will you ensure system access privileges aren't abused?

What does the change management process look like for bots?

How are impacted stakeholders educated on robotics?

What are the responsibilities of managers that control the bots?

*In these questions, the term "bot" refers to a smart automation technology that can be driven by either rule-based or cognitive intelligence–driven algorithms.

Addressing the current digitalization environment

Key risks associated with automation

When introducing these RPA and CI technologies into the ecosystem, enterprises are exposing themselves to potential risks that need to be addressed. We classify these risks into five key categories (see figure 3):
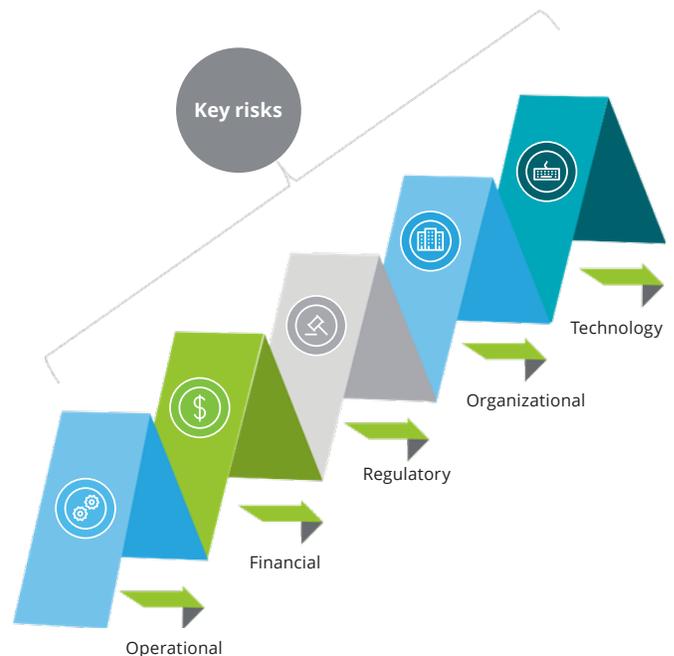
Operational risks:

- Poorly designed RPA and CI technologies, coupled with the high execution speed of bots, can multiply processing errors.

- Ineffective bot oversight procedures can lead to high-impact operational errors.

- Disparate approaches for applying RPA and CI technologies to business problems can lead to a non-standardized environment and increase complexity with the oversight of bots.

- Input data provided by developers to train the algorithms used for CI technologies may be incomplete, outdated, or biased. Or it may have an insufficiently large and diverse sample size. Furthermore, inappropriate data collection methods may result in a mismatch between the data used for training the algorithm and the actual input data used for the operations.

- Flawed assumptions, inappropriate modeling techniques, coding errors, and overfitting of automation algorithms to training data can present more operational risk.

- Many RPA and CI technology vendors are quite new and not fully mature, presenting third-party vendor and financial risk.

Figure 3. Five key risks associated with automation

Key risks

Technology

Organizational

Regulatory

Financial

Operational

Financial risks:

- Improper implementation of RPA and CI technologies can result in financial and reputational losses to the organization.

- Financial misstatements due to misalignment or misconfiguration of RPA and CI technologies may result in significant deficiencies or material weaknesses in internal controls over financial reporting.

Regulatory risks:

- A change in law or regulation can materially impact early adopters of RPA and CI technologies.

- Some highly regulated processes (e.g., data privacy) may be "off limits" for bot automation.

- Incorrect and/or incomplete regulatory reports generated through RPA and CI may result in regulatory issues and expensive fines.

- Bots may act in ways that contravene existing laws (e.g., learning algorithms may result in illegal discrimination against minorities).

- Data privacy standards and regulations may be at risk of noncompliance if the software bots used to collect confidential or restricted information aren't implemented with strict protection controls.

Organizational risks:

- The replacement or repurposing of full-time employees (FTEs) may negatively impact employee morale.

- Misalignment across groups may lead to gaps in roles and accountability.

- Missing standards around executing changes to bots may impede change management processes.

- A single bot may be equivalent to multiple FTEs, resulting in concentration risk.

- The nascent deployment of bots may introduce training challenges among stakeholders.

Technology risks:

- The impact of routine maintenance changes to the existing IT platform may need to be regression tested for dependent robotics implementations.

- The "black box" reality of the automation algorithms limits transparency into the workings of the technology.

- A software bot will require credentials to access data, systems, and applications. And like any other system user, a bot can present information security and access control challenges.

- Bots may be used inappropriately to perform tasks or scrape data from the applications. They're also more susceptible to a number of cyber attacks at the hardware, firmware, or application level.

- Business continuity and disaster recovery (BCDR) programs must account for the risks that the implementation of advanced analytics, RPA, and CI technologies present.

- Data provided to train a bot can be incomplete, outdated, or irrelevant, resulting in an incorrect outcome.

- Improperly designed bots working faster than agreed-upon SLAs may overwhelm existing IT systems.
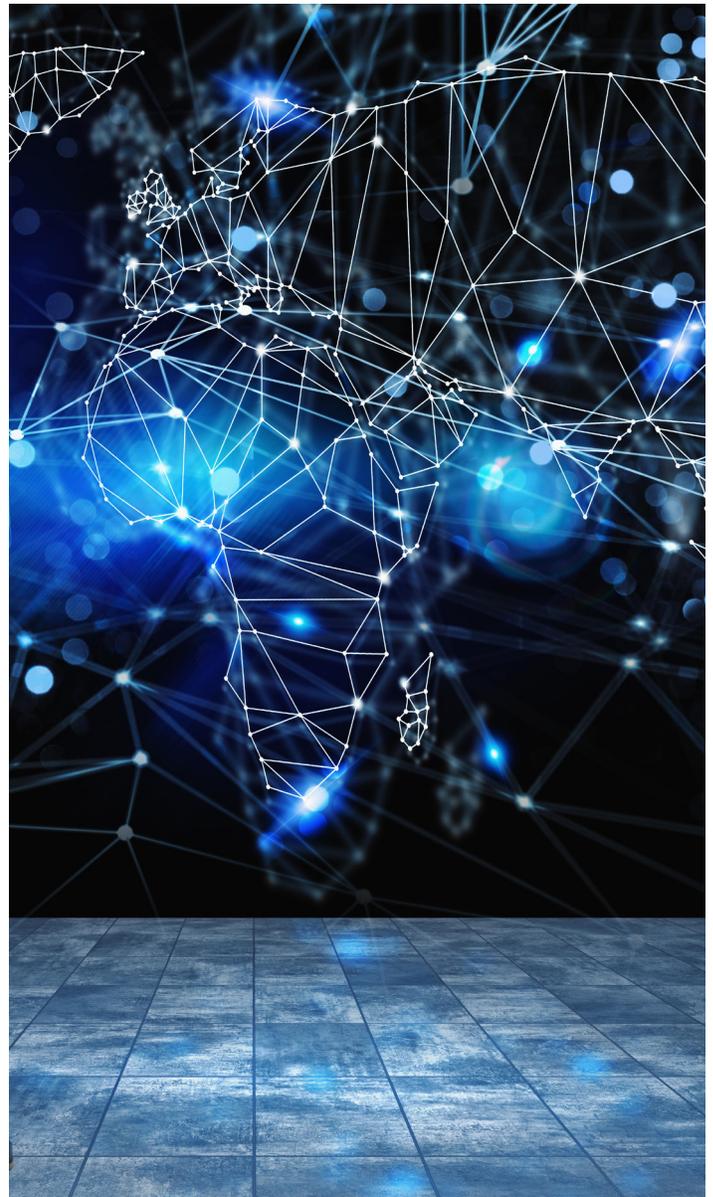
# Master the art of auditing risks due to digitalization

Assessing the impact of RPA and CI technologies on the existing controls environment, including new risks, is imperative to the successful adoption of these new-age technologies. But there's no need to reinvent the wheel. These risks can be addressed by extending existing approaches to managing enterprise risk. When assessing these technologies, IA should find a balance among their responsibilities to:

Assure: Providing traditional assurance

Advise: Acting as a trusted adviser

Anticipate: Preparing for new risks on the horizon

This balance is dependent on both the organization's maturity level of adoption and the strategic goals of the IA department.
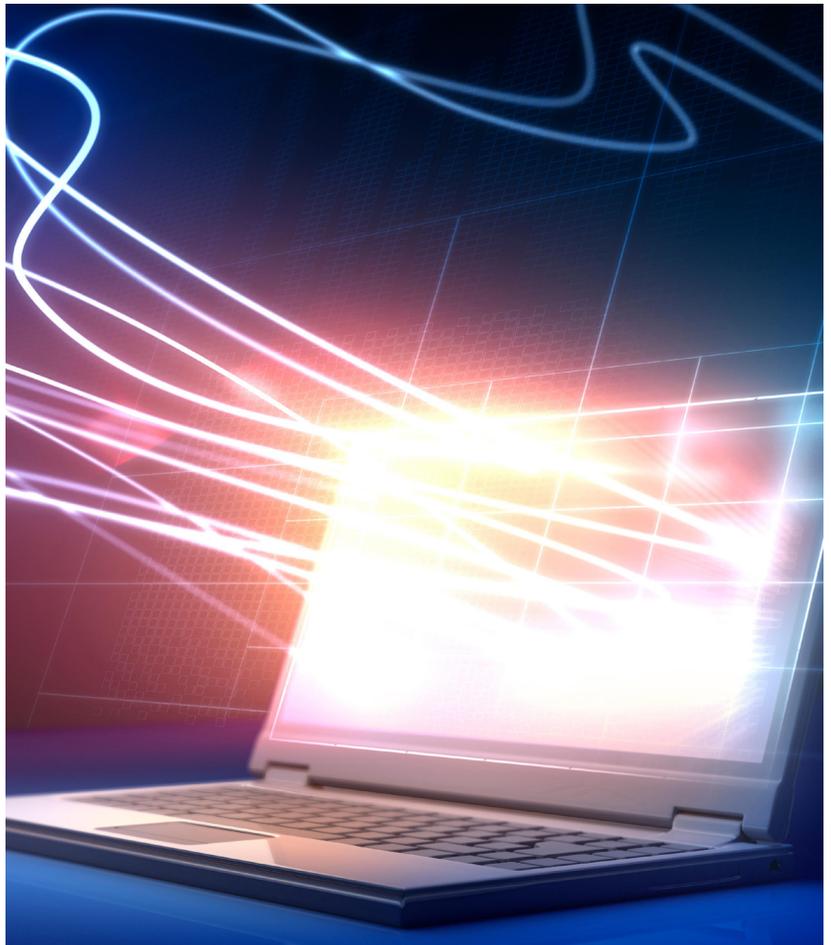
Go beyond controls and compliance. Offer actionable insights to build resilience and create value

+ Assure
Confidence

+ Anticipate
Foresight

+ Advise
Insight

Assure

The risks presented throughout the bot development life cycle (as shown in figure 4) are not necessarily new. They are merely an extension of a typical IT risk management framework. As the second line of defense (e.g., compliance and operation risk departments) pushes to modernize its approach for controls testing, and as many organizations move toward the combined assurance model to gain efficiencies, it is imperative for IA to get involved early in the journey. This will help IA provide effective and valuable assurance that is not duplicative.

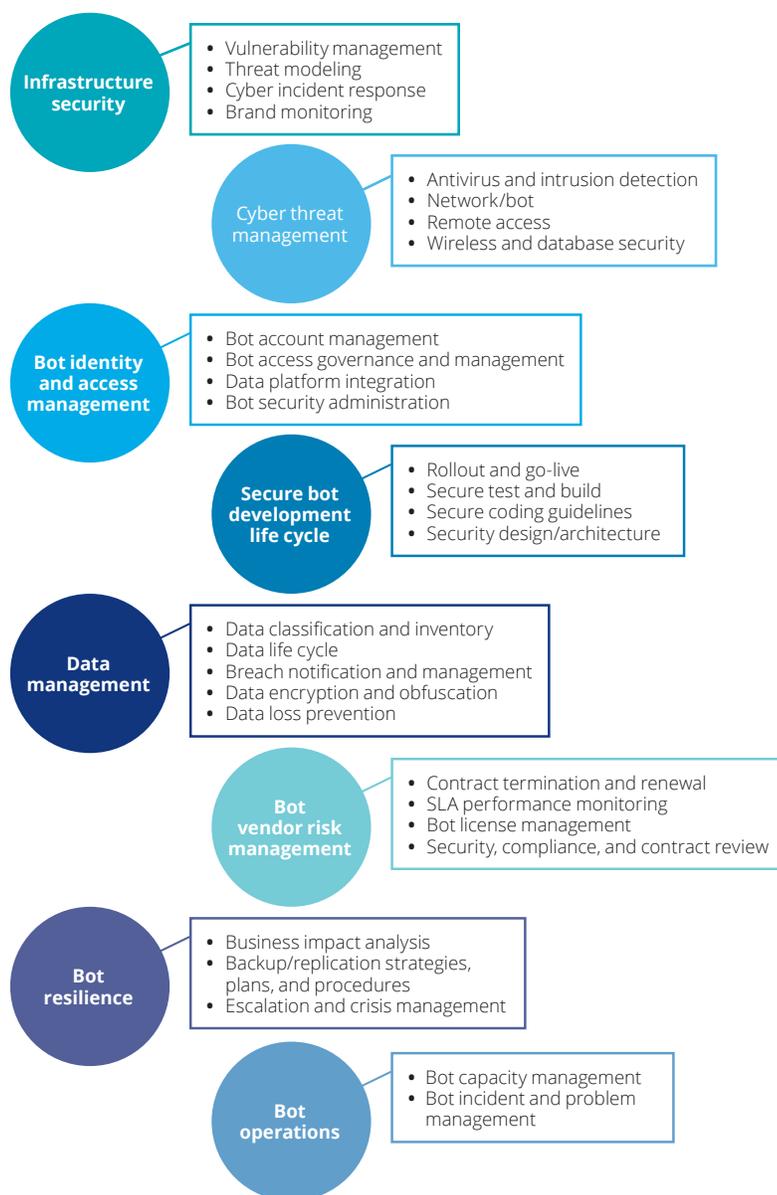Some practical considerations for IA to add value in providing assurance include:

Testing: IA departments should have access to the documentation of testing procedures and independently review the testing performed by sampling test cases documented, results generated, and issues logged.

Exception handling and monitoring: A framework and process should be designed to monitor the bots in testing and production environments, as well as triage issues that may arise. IA can consider the following elements of the framework as it proceeds to provide assurance on the design and operating effectiveness of bots:

- **Bot issue identification and resolution:** Are there tools and processes used by the business to monitor the quality of bot outputs, notify personnel of exceptions, and create predefined action plans to resolve and restore services in the event a bot execution fails?

- **Bot change management:** Is there a standard process for executing changes to existing bots, including notifying stakeholders and updating procedures and bot configurations?

- **Third-party risk management:** Do the automation software vendor contracts align with existing protocols for third-party technology vendors?

- **Business continuity:** Does the enhanced business continuity and IT disaster recovery plan include steps required to resume operations driven by the bot-based digital workforce?

- **Bot supervision and compliance:** How do bot owners and compliance personnel who oversee the work performed by bots ensure that bots adhere to the regulatory requirements and firm policies?

Recertification process: IA should encourage business and technology stakeholders to perform an annual recertification of the design and implementation of RPA and CI smart automation technologies. If necessary, the process should also be tested to provide objective assurance as to whether they are executing as intended.

Figure 4. Representative bot life cycle management events and sub-activities[2]

Infrastructure security
- Vulnerability management
- Threat modeling
- Cyber incident response
- Brand monitoring

Cyber threat management
- Antivirus and intrusion detection
- Network/bot
- Remote access
- Wireless and database security

Bot identity and access management
- Bot account management
- Bot access governance and management
- Data platform integration
- Bot security administration

Secure bot development life cycle
- Rollout and go-live
- Secure test and build
- Secure coding guidelines
- Security design/architecture

Data management
- Data classification and inventory
- Data life cycle
- Breach notification and management
- Data encryption and obfuscation
- Data loss prevention

Bot vendor risk management
- Contract termination and renewal
- SLA performance monitoring
- Bot license management
- Security, compliance, and contract review

Bot resilience
- Business impact analysis
- Backup/replication strategies, plans, and procedures
- Escalation and crisis management

Bot operations
- Bot capacity management
- Bot incident and problem management

---

[2] For information about additional algorithms risks, read "Managing algorithmic risks: Safeguarding the use of complex algorithms and machine learning," Deloitte Development LLC, 2017 https://www2.deloitte.com/us/en/pages/risk/articles/algorithmic-machine-learning-risk-management.html.

Advise

If organizations are in exploratory phases with the adoption of RPA and CI technologies, IA departments should get involved during the pre-implementation phase of RPA and CI automation. A few considerations for IA departments to bring to the table include:

- Advise the organization on its ability to account for risk factors involved

- Provide guidance on leading practices for driving greater performance and value

- Elevate IA's profile, demonstrating knowledge about the subject while maintaining objectivity

Some practical considerations to help IA elevate its role as a trusted adviser include:

Process documentation: IA should encourage business units to create and maintain pre-implementation documentation that can be easily audited. Examples of process documentation include:

- **Automation strategy:** Overall business value proposition, scope, resource (cost, staff) rationalization, and metrics to measure ROI and value

- **Automation process documentation:** Detailed procedures, from sampling to reporting, to aid in coding completion for the automation process

- **Automation process flow:** A visual representation of the overall robotics process

- **RPA coding for automation:** Detailed coding scripts covering end-to-end RPA for each test

- **Testing work papers:** This includes sample population, exception reporting, testing results, and final testing results/summary

Disseminate changes in the risk assessment process: IA should adapt a continuous risk assessment process to be able to evaluate innovation impact on a timely basis. To that end, IA should consider and integrate technological changes into the risk assessment process.

Execute dynamic audit procedures: IA should gear up to execute dynamic and effective audits more frequently, especially where bots are deployed on a large scale across a wide variety of use cases. IA may consider performing audits using an agile framework. If adopted correctly, the Agile Internal Audit framework promotes performing work in small increments, time boxed for a short duration, and focuses on collaboration to incorporate frequent feedback and improve audits iteratively.

Consider updates to reporting: IA should identify the level and structure of reporting required for RPA and CI automation audits (e.g., technology level versus business function level or assurance-driven versus consultative).

Anticipate

No matter what the organization's maturity level with respect to the adoption of disruptive digitalization, it is imperative for IA departments to anticipate and align efforts to monitor emerging risks, develop strategies, and implement risk remediation techniques. Analytics and new technologies enable IA departments to deliver insightful, proactive, and future-focused insights.

In addition to advising and providing assurance, IA should focus on anticipating emerging risks associated with RPA and CI automation technologies.

A balance between pushing the frontiers and risk appetite: In order to have a seat at the table and have a point of view in setting the risk strategy for disruptive technologies, IA should proactively understand the use case of each RPA and CI automated solution. IA should set a prioritization framework for auditing key risks, such as cyber and third-party risk, posed by the implementation of disruptive technologies.

Risk sensing and analytics: In anticipation of the implementation of RPA and CI technologies, IA departments should incorporate data analytics and risk-sensing tools to proactively identify emerging risks and gain insights on the best approach for auditing these new technologies.

Crisis simulations and early warning systems: Running a simulation using orchestrated crisis scenarios where a software bot implementation has gone wrong can help IA departments immerse themselves in their roles in real time. It can also allow them to reveal lapses in their organization's response capability at multiple levels: strategic, behavioral, and tactical.

IA must keep pace

As companies continue to adopt disruptive technologies in order to gain tangible operational efficiencies, IA departments need to keep pace. Here are some practical considerations for how IA departments can contribute:

Strategic planning and alignment: IA departments should create the strategic vision, goals, and road map on how they plan to audit processes that will be automated via RPA and CI technologies and advanced analytics. Their approach should define the audit selection methodology of these processes (high risk, frequency), sampling method, work paper templates, and issue resolution procedures. Furthermore, the vision should align and integrate with the existing enterprise risk management (ERM) framework and incorporate the overall strategic vision of the organization.

Risk assessments: IA departments should begin the risk assessment of RPA and CI automation as early on as possible. Based on the assessment performed, IA departments will be better able to gauge vulnerabilities and target areas for prioritizing audits. Due to the rate of technological advances and adaption, it's critical that IA assess the risk associated with digitalization continuously (see figure 5).
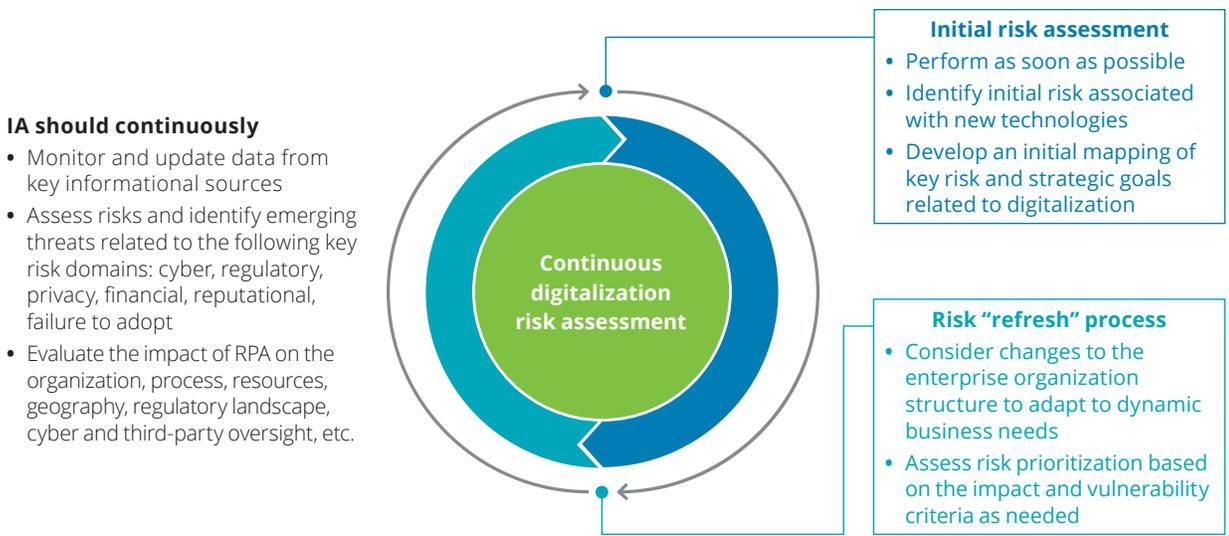
Analytics and dashboards: Leveraging analytics to design dashboards that provide IA departments with a detailed picture of the health factors of the RPA and CI technologies will help IA stay ahead of the curve.

Training and recruitment: IA professionals must adopt and adapt to the impending automation change. Understanding the nuances of these automation technologies can equip auditors with tools to perform their jobs more effectively.

In addition, senior management should inject fresh perspectives and knowledge by recruiting subject matter specialists from other departments or other companies. It's important for IA resources to have technical knowledge with respect to the technologies they are assessing, as well as a general understanding of the IA methodology they will be required to apply.

The power of automation: Last but not least, IA departments should consider opportunities to leverage advanced analytics and RPA and CI technologies to automate the audit life cycle, including audit risk assessments, audit planning, audit fieldwork, work paper documentation, and reporting. This not only allows IA departments to modernize their approaches to perform audits, but it also brings key insights on the challenges and risks posed by adopting these disruptive technologies.

Figure 5. Continuous digitalization risk assessment

IA should continuously
- Monitor and update data from key informational sources
- Assess risks and identify emerging threats related to the following key risk domains: cyber, regulatory, privacy, financial, reputational, failure to adopt
- Evaluate the impact of RPA on the organization, process, resources, geography, regulatory landscape, cyber and third-party oversight, etc.

Continuous digitalization risk assessment

Initial risk assessment
- Perform as soon as possible
- Identify initial risk associated with new technologies
- Develop an initial mapping of key risk and strategic goals related to digitalization

Risk "refresh" process
- Consider changes to the enterprise organization structure to adapt to dynamic business needs
- Assess risk prioritization based on the impact and vulnerability criteria as needed

Keep pace with disruption

The rate of adoption of disruptive digitalization technologies may be different for each company. Therefore, the preparedness level of each IA department to respond to the risks posed will vary. But the overall challenge remains the same: Get comfortable with discomfort. And brush up on what IA can do to deliver assurance and advise in the age of digitalization.

Deloitte Risk and Financial Advisory's globally recognized practice can help you manage and prepare for disruption. Our people, tools, and processes offer strategic solutions to assist you in understanding and auditing risks associated with RPA and CI technologies, as well as predictive data analytics. Disruption is here to stay— tapping into our experience can help you keep pace.

Contacts

For more information on auditing the risks of disruptive technologies, please contact our Deloitte Risk and Financial Advisory team:

Sandy Pundmann
US Managing Partner, Internal Audit
Deloitte & Touche LLP
+1 312 486 3790
spundmann@deloitte.com

Michael Schor
Partner, Internal Audit Innovation and Automation
Deloitte & Touche LLP
+1 212 436 6208
mschor@deloitte.com

Neil White
Principal, Global IA Analytics Leader
Deloitte & Touche LLP
+1 212 436 5822
nwhite@deloitte.com

Geoffrey Kovesdy
Senior Manager, Internal Audit
Deloitte & Touche LLP
+1 212 436 5149
gkovesdy@deloitte.com

Deloitte.