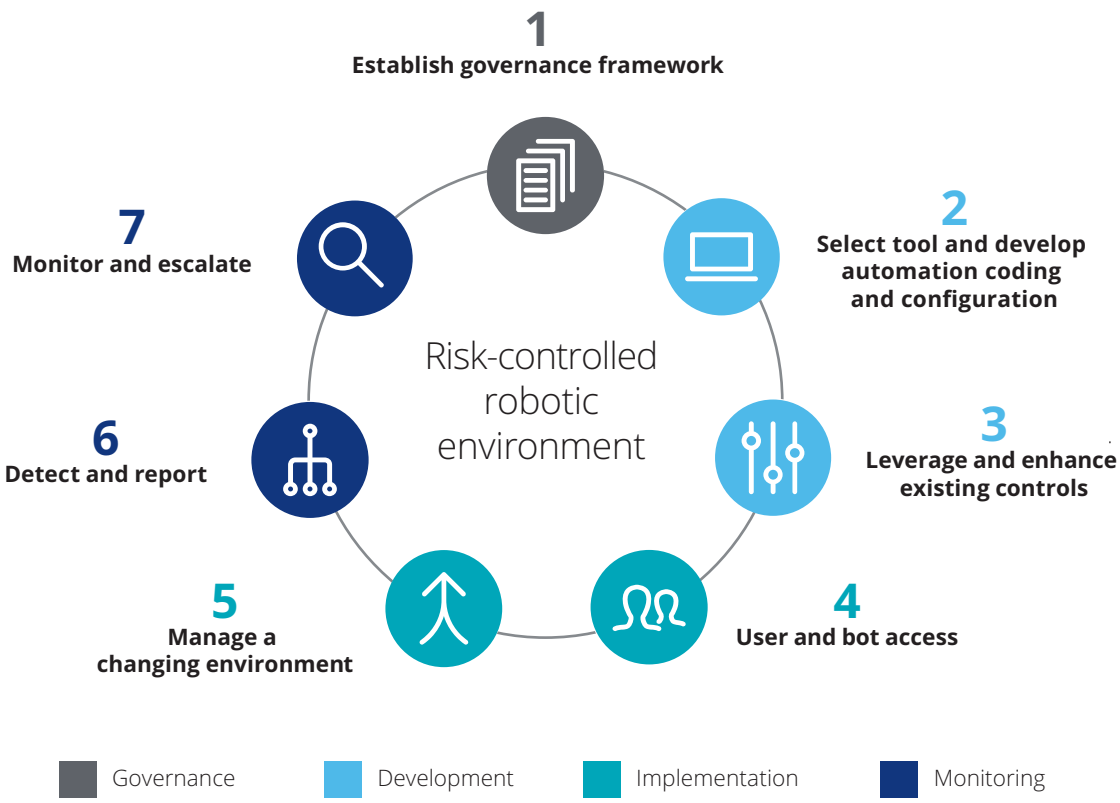
Deloitte.

Creating an environment for apt and adept automation

Seven-step progression of RPA risks and controls

Seven-step progression of RPA risks and controls



Companies across all industries are working to digitize parts of their business with robotic process automation (RPA), which is a platform where processes can be automated through the use of digital workers, often referred to as "bots." RPA programs use computer-coded, rules-based software bots to replicate the actions that a human would take to complete a computer-based task. The goal is to make the execution of simple tasks more efficient and effective, freeing up human capital to focus on more strategic priorities.

Gartner projects spending for RPA software to reach more than $2 billion in 2022.[1] Forrester, meanwhile, has predicted the RPA software market to total $2.9 billion in 2021.[2] With such rapid growth and widespread adoption, companies are advised to strike the right balance between innovation and risk. As RPA programs provide platforms that enable companies to move further along the automation spectrum toward more intelligent automation, leveraging cognitive capabilities such as machine learning and optical character recognition (OCR), there is even a further need to understand the appropriate level of risk with technology adoption. What is less known are the risks associated with RPA and the system of internal control needed to achieve the desired quality and governance necessary to deploy bots effectively. Outlined herein are the seven key steps to building a risk-controlled robotic environment.

1. Gloria Omale, "Gartner Predicts Up to Two-Thirds of iPaaS Vendors Will Not Survive By 2023," Gartner, March 7, 2019, https://www.gartner.com/en/newsroom/press-releases/2019-03-07-gartner-predicts-up-to-two-thirds-of-ipaas-vendors-wi.
2. Craig Le Clair, Alex Cullen, and Madeline King, "The RPA Market Will Reach $2.9 Billion By 2021," Forrester, February 13, 2017, https://www.forrester.com/report/The+RPA+Market+Will+Reach+29+Billion+By+2021/-/E-RES137229.

1 | Establish a governance framework

An RPA program depends on an appropriate governance framework inclusive of an overall automation strategy. The clearly defined, well-documented processes and controls of an effective governance operating framework directly affect an organization's ability to address the financial and operational risks surrounding the adoption of bots.

We often see the need for separate processes and controls around RPA, since many of the existing controls inhibit RPA usage or decrease the benefit of RPA (Deloitte's perspective on financial reporting RPA risks and controls[3] discusses how those charged with governance might outline and develop a corporate RPA charter that serves several important purposes).

RPA requires a low investment relative to other transformative technologies and offers the ability to automate mundane, repetitive tasks that absorb significant organizational resources. This leads to many organizations starting their RPA journey, but struggling to scale beyond the proof-of-concept phase. The root cause of this stagnation? A lack of a clear RPA vision and its related risks.

The level of investment in the strategy and vision phase directly affects an organization's ability to scale during ensuing phases and achieve a maximum return on investment. Based on observations from the front lines of our clients' RPA deployments, organizations who have overcome this barrier to scale have applied these three critical characteristics:

Reengineered business processes

There is a critical difference between asking "How can RPA fit into my current process?" and "How can I reimagine, rethink, and reengineer my current processes to take full advantage of RPA?"

A broken process should not be automated. Business process reengineering (BPR) and RPA should be viewed in conjunction with one another in order to maximize automation opportunities. A lack of standardization in the RPA process can lead to companies struggling to find higher returns on investment. Companies who achieve scale are able to perform RPA opportunity assessments as they rethink and redesign the way work is done.

This discover phase is when the foundation for digital risk management should be laid. Companies who deploy BPR with RPA can ask specific, risk-related questions, such as:

- ***Will reimagining my future-state process for automation create additional risks not yet mapped in the current state process?***
- ***Are there regulatory or compliance requirements that now come into play with automation?***
- ***Are there business risks associated with adopting automation that need to be effectively communicated to the organization today?***

IT incorporation

RPA is a business-led, information technology (IT)–supported program. Companies who scale involve IT early on in their RPA journey. Failure to provision access, institute change management control, and install appropriate development and test environments can result in risks and delays between the discovery and implementation phases of the RPA life cycle. IT's resources are vital in making sure RPA is installed properly.

Including IT during the initial discovery phase allows for proper planning of data security, change management, and access that aligns with existing policies and procedures. This minimizes risks related to IT general control and cybersecurity.

Cross-functional communication

A transformative RPA program requires collaboration between business, IT, human resources (HR), finance, internal audit (IA), and RPA stakeholders, and a clear digital strategy set by RPA program leadership. Companies who achieve scale and minimized risk are often able to form governance frameworks to effectively communicate a strategy and overall roadmap for RPA.

IA and HR are vital to addressing RPA risks. IA can help management vet potential RPA opportunities identified during the discovery phase while keeping a risk and control framework in mind. HR can support workforce readiness while providing planning that incorporates digital employees and minimizing talent and accountability risks.

3. Deloitte, "Financial reporting RPA risks and controls: Considerations for developing and implementing bots," 2018, https://www2.deloitte.com/us/en/pages/audit/articles/financial-reporting-rpa-risks-and-controls.html

2 | Select tool and develop automation coding and configuration

As companies select their RPA platform, details of both the business and solution design requirements of relevant automation should be maintained, so internal and external auditors can perform appropriate automated control testing procedures. Companies that do not plan for appropriate documentation during the development of bots may create a gap in the system of internal control.

In addition to testing the system configuration, companies should plan to appropriately document test-case scenarios considering both positive and negative testing situations in an effort to test the coding and configuration underlying the bots. Once deployed to production, management should maintain appropriately sufficient documentation in order to test sample transactions and determine if the automated control operates consistently with the underlying program, code, and configuration.

3 | Leverage and enhance existing controls

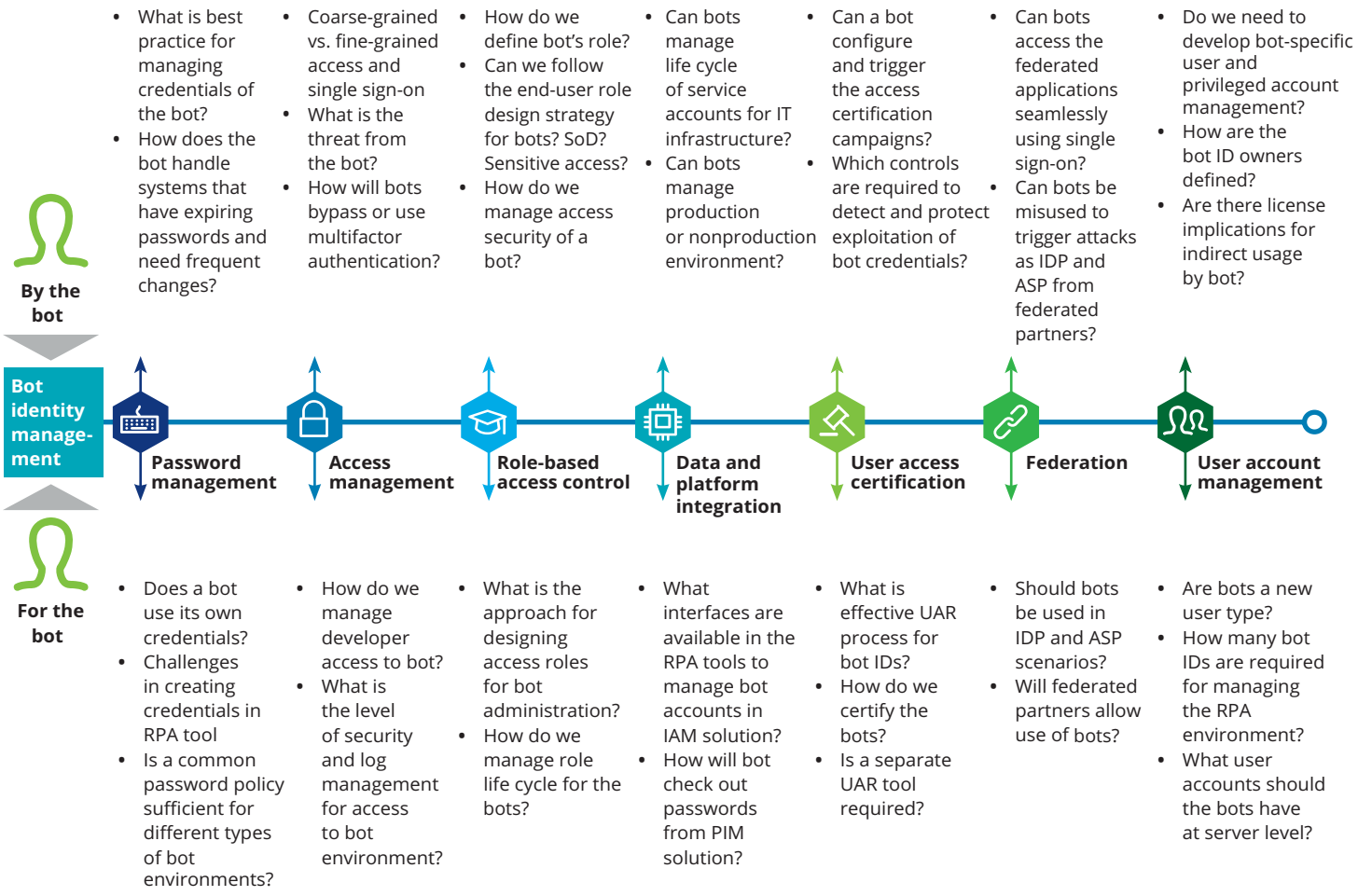
As companies develop bots, they should assess the impacts of the bot on its existing controls. After a bot begins operating, control activities are needed to address the risks of the designed automation not operating properly. Companies could benefit from having RPA controls, such as monitoring transactional logs and unexpected activities, to make sure the automated process is completed effectively. If existing controls cannot address the risks associated with bot implementation, companies should enhance those controls.

RPA users should also consider how the bot would affect its existing controls. If any of the existing controls are bypassed, appropriate approvals would need to be obtained. A bot that is not properly designed and developed could inadvertently change an existing control, or conversely, enable a better control by replacing manual processes with automation. An impact assessment can help companies avoid unintended SOX (Sarbanes-Oxley) compliance consequences and improve their system of internal control.

4 | User and bot access

Companies should think about their existing user access controls when implementing an RPA program. In a traditional IT environment, there are system IDs and end-user IDs. There are the same number of IDs as business roles. Whether companies decide to deploy automation representing "digital workers" or deploy a combination of "digital workers" and humans accessing the same IT systems, distinguishing between humans accessing and bots accessing IT systems becomes ever more important. Credentialing humans and bots representing the same worker becomes involved, and segregation of duties (SOD) becomes challenging. In these cases, identity access management (IAM) can provide a useful framework. As shown in the seven steps below, deploying traditional IAM requires end-user and system IDs to be segregated based on the nature of access and transactions handled. This scenario changes with the implementation of an RPA program. A bot can automate a process from end to end, which may encompass multiple business roles. Bots access systems like humans, but operate more like system IDs.

Companies should determine what modifications to their existing user access controls are required for them to continue to operate effectively in the bot world. Leveraging Deloitte's IAM Methods®[5] approach can help identify these RPA-specific challenges. The seven components of our IAM framework show additional considerations that should be made by a company when deploying bots.



5. Deloitte's IAM Methods®
https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-bot-identity-management-presentation-final-print-noexp.pdf

SOD is critical when implementing and monitoring RPA programs. Gartner[4] warned, "Through 2020, 25 percent of large enterprises will experience insider fraud, due to lack of proper SOD controls around RPA. The major source of fraud will be lack of SOD controls over the human actors who have authority over RPA identities. This will enable them to manipulate two or more SOD-compliant RPA identities that together can provide a toxic combination of entitlements."

While bots themselves do not have conflicting interests, a bot is managed by a human. Problems can arise when the manager's system access conflicts with the bot's system access or when a manager is responsible for multiple bots with conflicting system accesses. When documenting the process workflows during the development phase, companies should assess the combination of access rights and business roles granted to a bot and the human that controls them. This can confirm that all conflicts have been identified and mitigated and that all potential SOD violations are addressed prior to the deployment of bots.

5 | Manage a changing environment

Effective change management is critical to a company's RPA implementation. Existing change management frameworks should be extended to account for the existence of bots and to track the impacts of internal or external changes—things like system upgrades, change in service providers, change in process work flows, change in reporting requirements, and even changing schedules.

From a technology perspective, a change management program for a company deploying its first bots will be like programs in place for its software development life cycle. After an automation is designed, a company should do four things:

1. Complete user acceptance testing to confirm the automation is performing as designed
2. Transition the automation to the production environment and monitor
3. Monitor scheduled bots for break/fix issues and report performance metrics
4. Develop performance summary reports and implement performance improvements while operating the existing bots

Companies should determine the key performance indicators and metrics for measuring the value of the automations early in the RPA life cycle to confirm they set a baseline for measuring value over the long term.

The personnel aspect to implementing RPA should not be ignored. The replacement or repurposing of humans may negatively affect employee morale. Management should clearly communicate the company's digital strategy and its desired future state to confirm everyone understands RPA's purpose and benefits, as well as the complementary roles the workforce and bots play in the overall strategy.

4. Felix Gaehtgens et al., *Predicts 2018: Identity and Access Management*, Gartner, November 30, 2017, https://www.gartner.com/en/documents/3834576.

6 | Detect and report

When a bot fails, management should carefully evaluate these characteristics:

1. Nature of the failure, such as data processing or handling
2. Source information—did something change within the source data?
3. Magnitude of the failure—was there a downstream impact from a process standpoint?

The results of management's evaluation should not only be used to fix the issue with the bot's operation, but also to evaluate the related policies and procedures within their bot development process.

Because bots can generate enormous amounts of data within a relatively short period of time, management may also automate the generation of reports utilized within their existing monitoring controls. Therein lies the new opportunity.

As an example, we can look at a weekly or monthly inventory production management meeting. Typically, these meetings include individuals responsible for separate portions of the business process—a floor supervisor, an inventory manager, and a quality assurance representative. Management evaluates information obtained in the meeting to identify anomalies that may indicate that controls within the process are not in place or are not functioning properly. This information may live across multiple systems and require significant organization and formatting before management can perform its review. That is a task particularly well-suited for RPA.

7 | Monitor and escalate

RPA's impact on management's monitoring is twofold:

- **New responsibility:** Monitoring digital workers and their output within the existing system of internal control
- **New opportunity:** Utilizing RPA to enhance existing monitoring controls

When it comes to that new responsibility, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) breaks down the monitoring component into two principles:

1. Ongoing and/or separate evaluation(s) of internal control performance
2. Evaluation and communication of deficiencies

The evaluation principle should be relatively simple to integrate within an RPA strategy. Most RPA platforms provide users with the ability to generate bot operating statistics and define key performance indicators associated with bot operation. Detecting routine bot failures in real time allows for management awareness prior to a result being produced. Additionally, performance metrics defined during the development process can summarize the value generated by an automation simply by tracking the number of runs.

The results of a company's ongoing and/or separate evaluations of bot performance should inform management as to when there may be a deficiency in their control environment. Management is expected to maintain appropriately designed and effective general IT controls for the relevant IT components associated with a digital worker, as well as policies and procedures around process governance in which bots are utilized.

A framework you can count on

The opportunities for efficiency and resource redeployment that RPA technology can provide are essential to the future growth of many companies. RPA and other emerging technologies are laying the foundation for how the future of work will be performed.

We do not believe these technologies will replace humans, but we do believe that humans who leverage these technologies will replace humans who do not. To reap these benefits, companies should establish a well-organized and agile RPA governance framework enabling them to identify RPA risks and resolve them under an appropriate controls environment, which is no simple task.

The processes and controls that bots can take over might be mundane, but the support structures they operate within certainly are not.

Authors

Cameron Andriola
Audit & Assurance Manager
Deloitte & Touche LLP
+1 702 893 5148
candriola@deloitte.com

Helen Deng
Audit & Assurance Senior Manager
Deloitte & Touche LLP
+1 713 982 2169
xiadeng@deloitte.com

Chris Spraberry
Audit & Assurance Senior Manager
Deloitte & Touche LLP
+1 504 561 7135
cspraberry@deloitte.com

Stefan Elliot Ozer
Audit & Assurance Senior Manager
Deloitte & Touche LLP
+1 203 423 4731
sozer@deloitte.com

Ginny Coulter
Audit & Assurance Senior Manager
Deloitte & Touche LLP
+1 713 982 2349
gcoulter@deloitte.com

Review contributors

Scott Szalony
Audit & Assurance Partner
Deloitte & Touche LLP
+1 248 345 7963
sszalony@deloitte.com

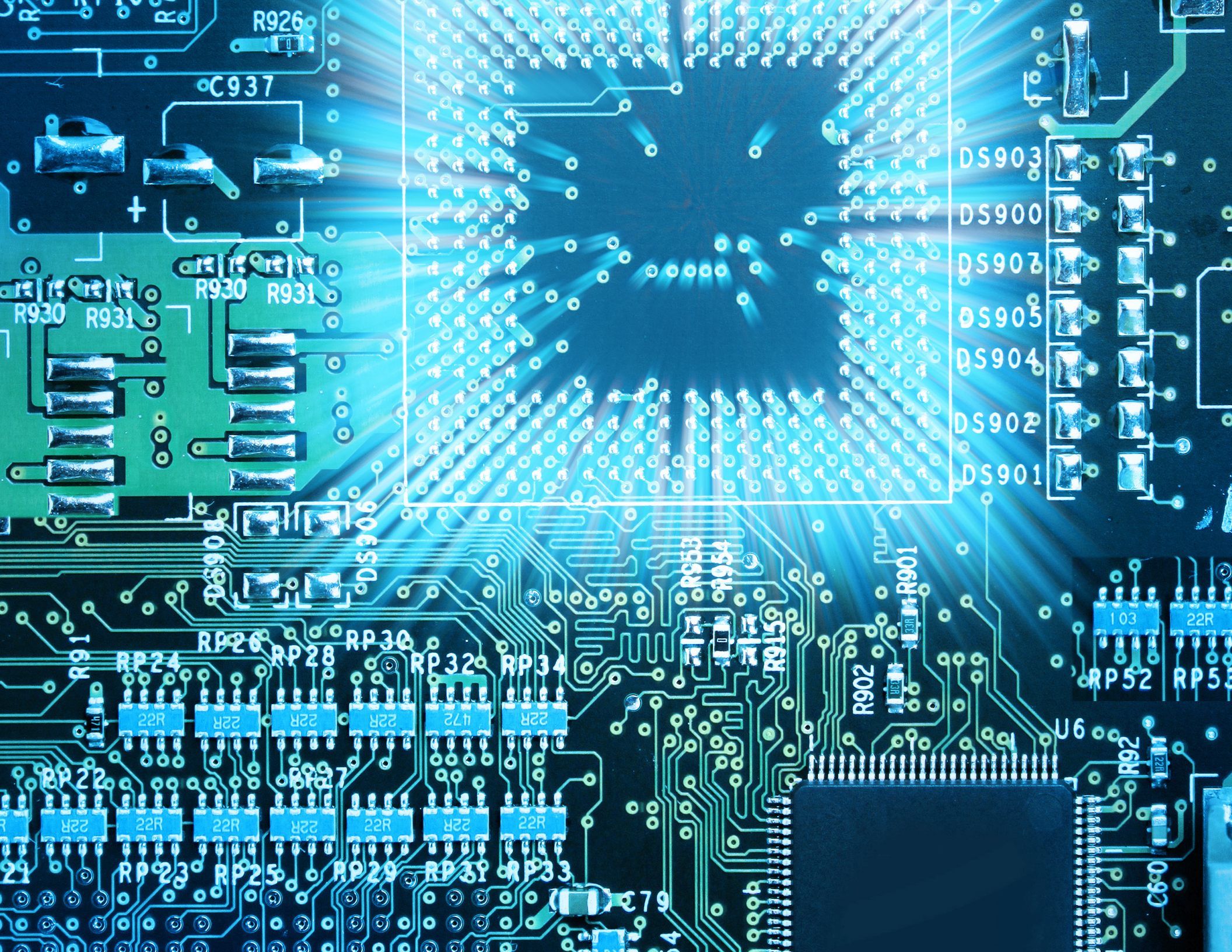
Isa Farhat
Advisory Partner
Deloitte & Touche LLP
+1 703 251 1109
ifarhat@deloitte.com

Kirti Parakh
Audit & Assurance Senior Manager
Deloitte & Touche LLP
+1 312 513 8006
kirtiparakh@deloitte.com

Valeriy Dokshukin
Advisory Partner
Deloitte & Touche LLP
+1 303 305 4858
vdokshukin@deloitte.com

Kyle Sewell
Audit & Assurance Senior Manager
Deloitte & Touche LLP
+1 404 201 0759
ksewell@deloitte.com

Jeffery Aughton assisted in the production of this publication.


R926
C937
R930
R931
R930
R931
DS903
DS900
DS907
DS905
DS904
DS902
DS901
DS906
DS908
R953
R954
R901
R915
R902
RP26
RP30
RP24
RP28
RP32
RP34
R91
RP22
RP27
RP23
RP25
RP29
RP31
RP33
C79
U6
RP52
RP53
103
22R

Deloitte.