KPMG

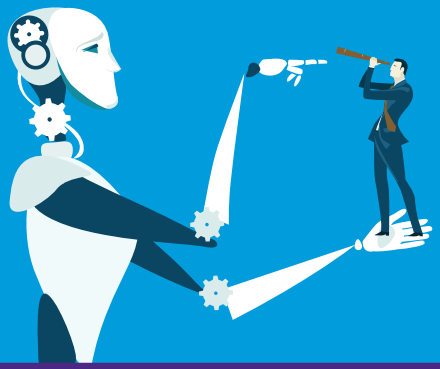
Managing risks of the growing RPA jungle

Balancing risk and change in Robotics Process Automation (RPA) transformation

KPMG.com/in

Table of contents

Rise of the virtual workforce



A recent study by Hfs Research and KPMG reports that

62 percent

of North American enterprises are looking at new opportunities available with RPA systems.

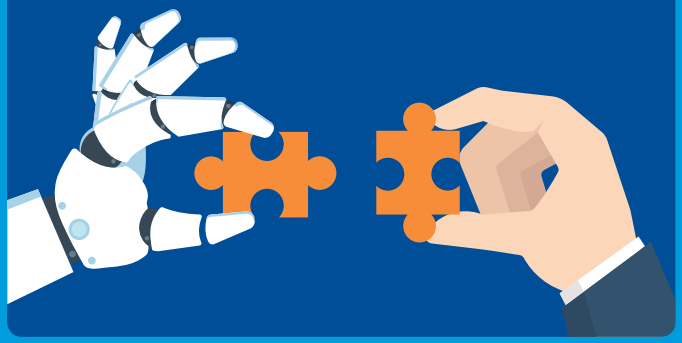
Global spend on Robotics Process Automation (RPA) is expected to increase at

60 percent

in coming years. In the next coming 35 years, Business proposition might drastically change by automation or hybrid solution.

Right from the 1990s, businesses achieved unprecedented levels of speed, accuracy, and cost efficiency by using technology to do so much more than what a human workforce could. Recently, a transition to Robotic Process Automation (RPA) and artificial intelligence-driven cognitive automation to transform businesses is one of the foremost game-changers among the emerging technologies.

The Institute for Robotic Process Automation and Artificial Intelligence[1] (IRPAAI) defines **RPA** as the application of technology that allows employees in a company to configure **computer software or a robot (BOT)** to capture and interpret existing applications for processing a transaction, manipulating data, triggering responses and communicating with other digital systems.



1. https://irpaai.com/definition-and-benefits/, Institute for Robotic process Automation and Artificial Intelligence (IRPAAI), 2018

Organisations with a large scale as well as mid-size workforce will benefit from introduction of RPA as it can eliminate redundant tasks, boost capabilities and ultimately save money. But the reality is that even low scale organisations and entrepreneurs are showing interest in process optimisation through technologies like RPA. The Robotics and Intelligent Automation (RIA) spectrum is broadly divided into three categories with some capability overlap across categories: Basic RPA, Enhanced Process Automation and Cognitive Automation (IQ).

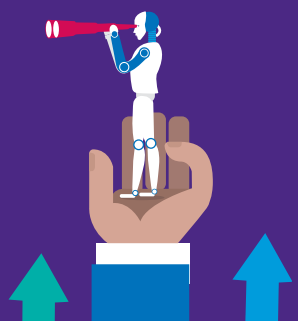
The first few to kickstart their process automation journey mostly ended in failure leading to reputational, financial, and legal damage. The management of companies then wondered:

- Was RPA a one-time, cost-effective solution constituting ideal mix of basic, enhanced and cognitive automation?
- Did we identify and evaluate all the risks and benefits involved in existing and future automation opportunities and what are the expected regulatory compliance requirements to adhere?
- Is there an effective business continuity plan in place in case of RPA failure?
- Most importantly, how important is it to identify in-house or external consultants who are Subject Matter Experts (SMEs) who can support the RPA transformation.

What is needed for a seamless transition?

In this point of view, we at KPMG are looking at what are the key considerations during the multiple phases of RPA implementation to identify and mitigate inherent, general technology and emerging IT risks. Over the past couple of years, we have implemented and reviewed multiple RPA programmes for clients, conducted a series of workshops, and undertaken research about the significant factors that impact business during/post the implementation of RPA.

Typical stages of RPA implementation and indicative risks in each stage



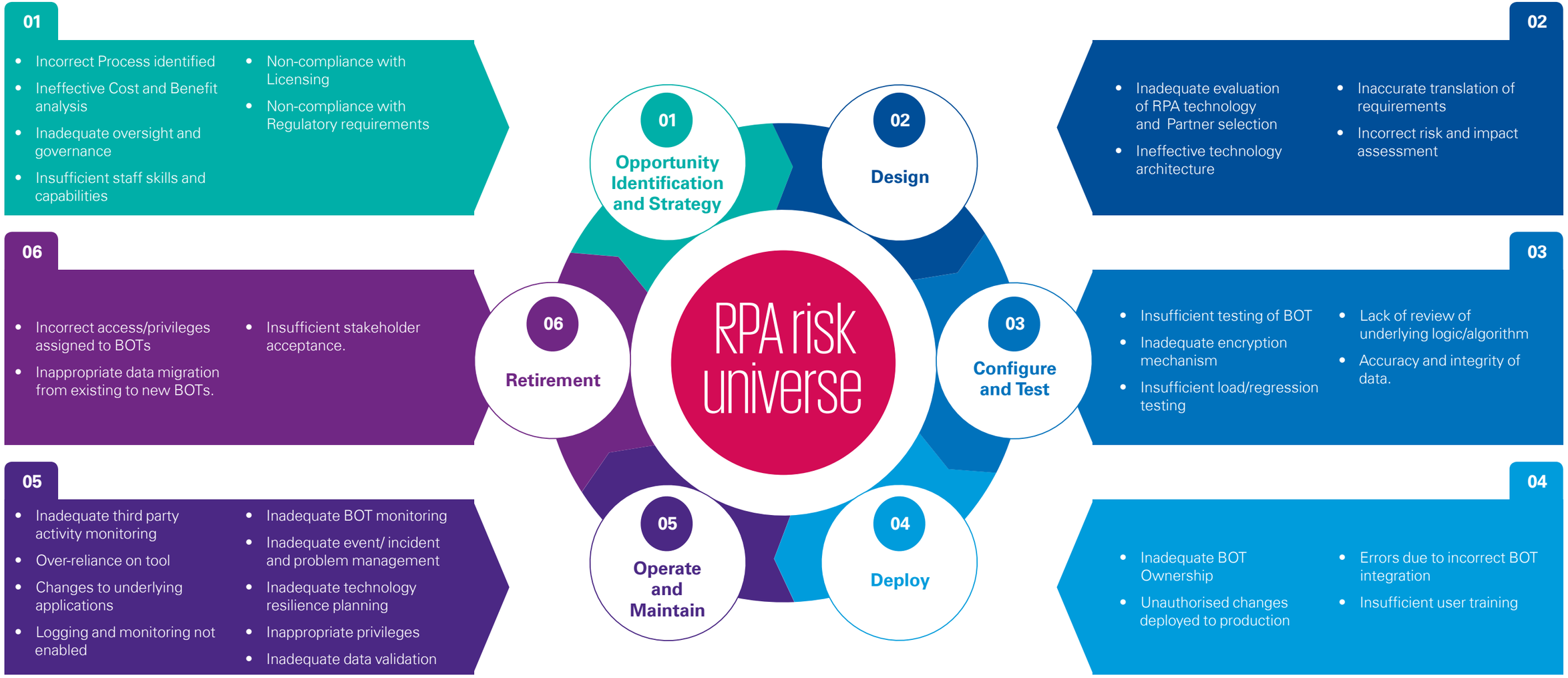
Many organisations have aggressively deployed RPA considering the modern management philosophy of cost effective business returns by automation; however they have treated the subsequent risks as a secondary concern. A defined, standardised and accountable risk governance mechanism for RPA programmes will be the pivotal source of competitive advantage for any business. It is highly critical for collaboration of Business and Technology teams with the Risk and Compliance teams to work on the overall governance of RPA programmes.

We have classified multiple stages of RPA implementation into six phases as mentioned below:

1. **Opportunity identification and strategy:** The initial stage of RPA implementation is to identify potential automation opportunity by systematically evaluating existing Business and IT processes. For a sustainable and compliance fulfilled model, ensure adequate RPA ownership, oversight and governance is in place.
2. **Solution design:** Perform review of target business processes and activities for automation enablement by selecting the right technology and partner for the opportunity. Develop and sign off future state processes and activities.
3. **Configure and test:** Configure the BOT via a scalable platform that allows users to plan each process graphically. To meet all business user requirements and ensure BOT performance is within acceptance criteria perform a structured testing process prior to implementation in production environment.
4. **Deploy:** Post to production readiness review, BOT is migrated as 'virtual workforce' in the production environment to perform automated processes
5. **Operate and maintain:** Monitor and review of the inter-connected runtime resources/BOT in the production environment by executing a governance and change management strategy. Conduct monitoring and reviewing of BOT and infrastructure for overall performance and compliance of RPA programme
6. **Retirement:** The final phase of RPA implementation is the process of shutting down and removing outdated and/or redundant BOTs from production environment. Business concludes on the decision to retire any particular BOTs after realizing they cannot support the business function/process.

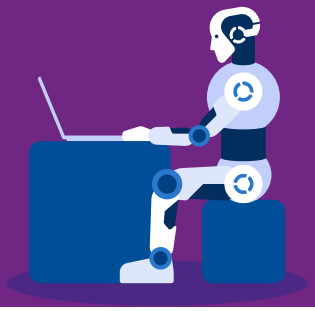
Key activities at each phase of RPA Implementation

Before transition, organisations must know an RPA programme has inherent risks. Let's look at illustrative risks across all the stages of RPA implementation.



© 2018 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Understanding the risks: Select cases



Drawing from our experience, here are a few examples where organisations have taken steps to facilitate RPA assessment.

Case 1: A global investment bank improves it processes with a Risk and Control Self-Assessment (RCSA)

The objective

KPMG was engaged to perform a Risk and Control Self-Assessment (RCSA) for RPA programme which included assessment of Automation Anywhere (AA) platform and underlying BOTs.

What were the benefits for the client?

The identified findings from assessment helps the management to formulate remediation action plans to address control gaps taking in account with risk and cost-benefit considerations. This resulted in process improvement opportunities to the management.

Case 2: A global investment bank achieves better process efficiency with assessment of RPA managed process

The objective

KPMG provided a detailed report for process improvement after conducting design and operating effectiveness review of RPA managed process considering operational and technology risk.

What were the benefits for the client?

A detailed review of design and operating effectiveness of BOTs implemented helps in determining risk free controlled production environment. The recommendation for process improvement achieve a process efficiency of 80 per cent and thus reducing the level of operational and technology risk exposure.

Case 3: Assist a global brewing company in framing a consolidated RPA risk and control framework

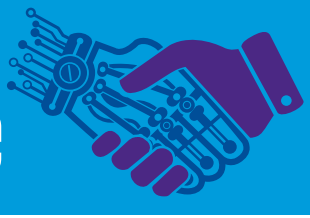
The objective

KPMG was engaged to create a customized RPA risk and control framework after understanding the financial impact of the RPA enabled processes factoring regulatory and governance considerations.

What were the benefits for the client?

The assessment provides awareness to stakeholders on identified gaps/deviations within the implemented BOTs (in RPA programme) and recommend the leading industry practices and regulatory requirements for enhancement. Thereafter framing a customized risk and control (governance) framework for on-going RPA development.

Recommended approach to manage key considerations in RPA programme



As process automation remains to be primary objective of an RPA programme, organisations have realised the necessity to establish accountable, sustainable, secure and compliant technology environment from the inception. To address these roadblocks, they should create an exclusive risk framework for the RPA programme to manage these considerations.

Based on our understanding, RPA programme specific assessment and governance framework (can be also called as BOT-assessment and governance framework) should be an all-inclusive matrix created factoring in inherent risks, emerging technology risks, information security, programme governance, regulatory considerations and industry best practices. The framework augments RPA programme for organisations during BOT implementation in identifying significant risks from various dimensions and designing controls to mitigate the risk.

RPA assessment & governance framework

Programme Governance

- Strategy and Governance
- Process Selection
- Ownership
- Business Continuity
- Tool and Third Party Selection
- Policies and Procedures
- People skill and Capabilities
- Licensing Compliance

Technology Risk

- Access Administration
- Logging and Monitoring
- Change Management
- Backup and Recovery
- Incident Management
- Development Management

Regulatory Considerations

- Applicable Regulations
- Local Law Considerations
- Leading Industry Standards and Framework

BOT Logic and Functionality

- Source Code Review
- Interface Testing
- Segregation of Functions
- Action – Intent Analysis
- Control Centre Review
- Exception Handling

Privacy and Security

- Privacy
- Vulnerability Management
- Data Encryption
- System Architecture

© 2018 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

A few fundamental questions that might arise during the assessment of an RPA programme:

BOT Logic and Functionality:

1. How does the BOT validate its input-output data?
2. Is there a mechanism to monitor BOT performance?
3. How is the segregation of functions maintained?

Privacy and Security:

1. What is the process of handling password vault management?
2. How are the passwords for BOT scripts managed?
3. Is input –output data encrypted to achieve effective data security?
4. Is there any Personal identifiable (PI) data involved?
5. Is there a vulnerability management programme covering the RPA landscape?

Regulatory Considerations:

1. Does the BOT have any regulatory/compliance (FISMA, SOX, GDPR etc.) implications?
2. Do vendors or third party associated in RPA programme adhere to compliance requirements?

Program Governance:

1. Does BOT implementation involves any signification changes or cross impact to the existing business environment?
2. Is BOT software license compliant?
3. Are all relevant stakeholders involved for automation requirement?
4. Are there defined SOPs to reflect the revised operating model?
5. Did the company provide trainings to scale up the skills of workforce to work in new Robotic environment?
6. Is there a defined BCP and DR plan?

Technology Risk:

1. How do you prevent toxic access pair (segregation of duties)?
2. Does the company maintain an inventory of BOT scripts?
3. Is there a defined roll back plan?
4. Does the company maintain an audit trail for BOTs activities and performance?
5. How is the change management process designed/structured for the BOTs?

Conclusion

Adoption of RPA has become a realistic solution intended to provide tactical benefits and allows organizations to concentrate on strategic solutions on a larger scale. Automation is the new norm in the business and the subsequent risk disrupt the innovation. With the future of business being managed using Artificial Intelligence (AI), Machine Learning and Deep Learning, auditing/assurance of these emerging technologies is becoming more complex than a customary technology audit.

This chapter of intelligent automation series will acts in providing awareness for identifying and managing risks during RPA programme for anyone interested in process automation. As a step forward, we would like to mention six quick recommendations to manage risks within RPA programme:

a. evaluate whether the automation solution is balancing value and risk to the business

b. setup an independent Governance and Oversight committee during the initial phase for secure business transformation

c. establish a RPA risk framework incorporating disruptive risks in dynamic environment

d. perform risk review and testing of RPA controls on a periodic basis

e. deep dive of theme-based reviews such as Privacy, Cyber Security testing, Regulatory review, etc.

f. develop utilities/tools to automate RPA controls testing.

Acknowledgements

Shabbir Tahasildar

Eesha Zutshi

Rahul Chandran

Nisha Fernandes

Rasesh Gajjar

KPMG in India contacts:

Nilaya Varma
Partner and Leader
Markets Enablement
T: +91 124 669 1000
E: nilaya@kpmg.com

Akhilesh Tuteja
Partner and Head
Risk Consulting
Co-leader - Global Cyber Security
T: +91 124 307 4800
E: atuteja@kpmg.com

Atul Gupta
Partner and Head
IT Advisory - Risk Consulting
National Leader - Cyber Security
T: +91 124 307 4134
E: atulgupta@kpmg.com

Abhijit Varma
Partner
IT Advisory - Risk Consulting
Leader - KPMG India Lighthouse
T: +91 803 065 4354
E: avarma@kpmg.com

Anil K V
Director
IT Advisory - Risk Consulting
National leader - IT Internal Audit
T: +91 803 065 4367
E: anilkv@kpmg.com

KPMG.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG in India 25 YEARS of making a difference