Deloitte.

Secured BOT Series

2018

Risk Management For and By the BOT
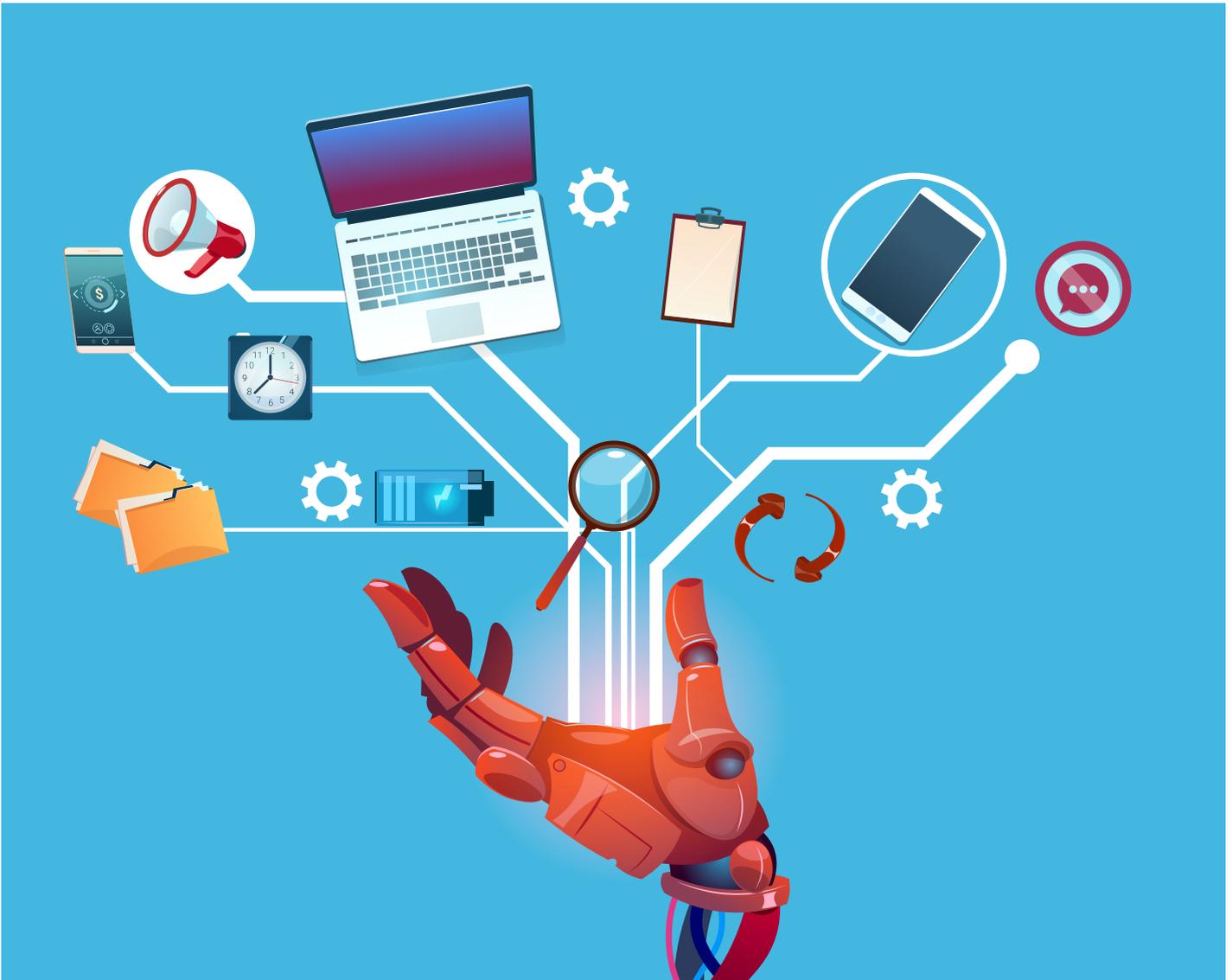
Secured BOT Series

2018

Contents

Risk Management For and By the BOT

RoBOTs have sooner become a reality than most of us thought. In the current avatar, Robots are making your business more responsive, cost effective, compliant and efficient. Many of us already see these digital clicks happening around us. We are already entering an era where BOTs are doing intelligent work and building efficiencies.

While technology makes our life efficient, it also opens new risks

to the business environment. A typical Robotics Process Automation (RPA) system design provisions interconnection between multiple systems and hence also has an impact on underlying system control environment.

Lets examine its relevance to business environments.

- **Opportunity:** Can you make your digital platforms more secured and compliant through RPA?
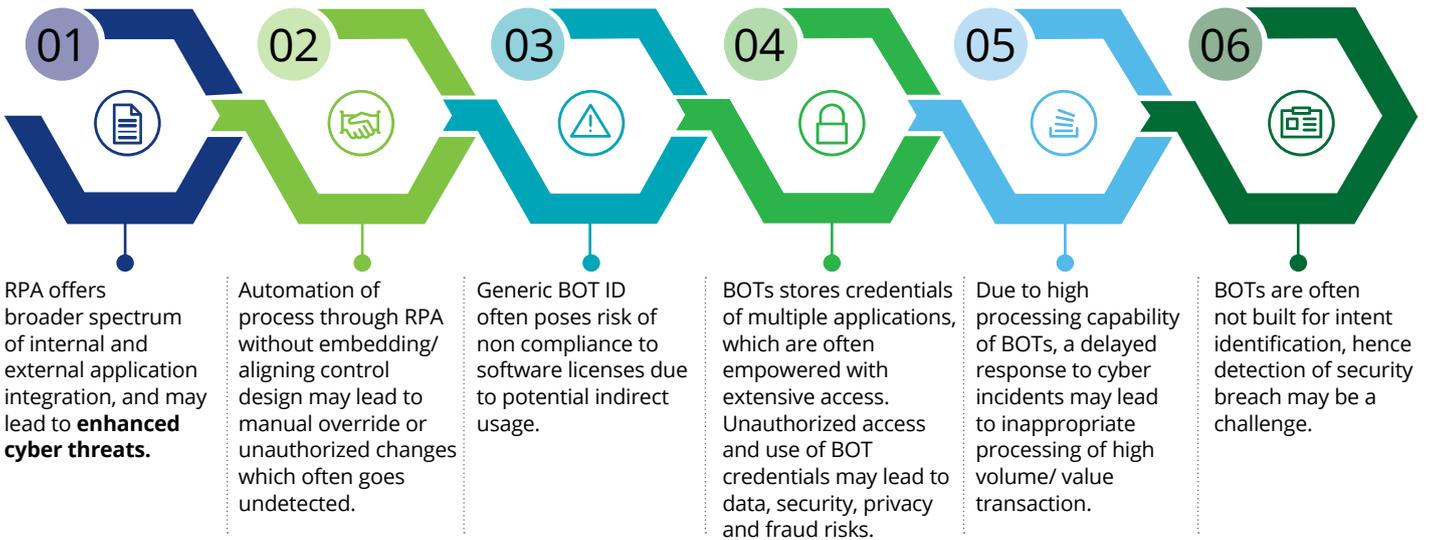
- **Threat:** How secured is your RPA environment from internal and external threats?

It is essential for an organization to build a secure BOT strategy when they move from a POC to Production environment.
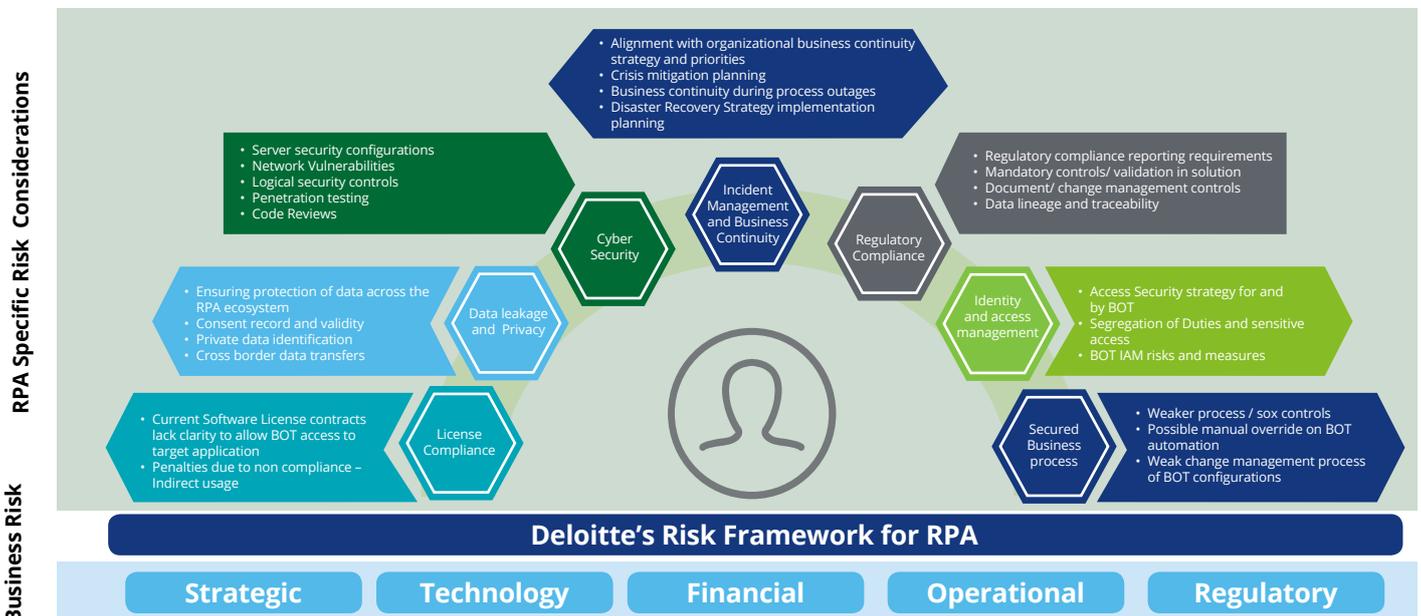
Setting context for RPA Risk Management

Typical risks in an RPA environment

RPA brings its own inherent risks as well the ones which are resultant of the business environment it automates.
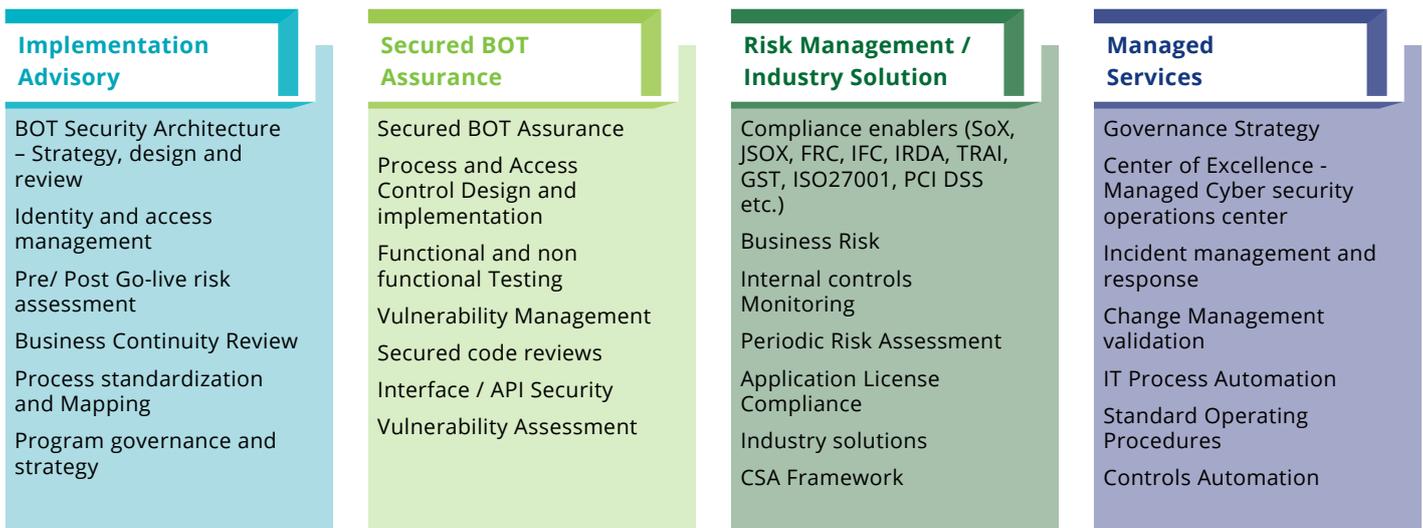
01
RPA offers broader spectrum of internal and external application integration, and may lead to **enhanced cyber threats.**

02
Automation of process through RPA without embedding/ aligning control design may lead to manual override or unauthorized changes which often goes undetected.

03
Generic BOT ID often poses risk of non compliance to software licenses due to potential indirect usage.

04
BOTs stores credentials of multiple applications, which are often empowered with extensive access. Unauthorized access and use of BOT credentials may lead to data, security, privacy and fraud risks.

05
Due to high processing capability of BOTs, a delayed response to cyber incidents may lead to inappropriate processing of high volume/ value transaction.

06
BOTs are often not built for intent identification, hence detection of security breach may be a challenge.

Deloitte's Risk Framework for RPA

A secured and compliant BOT environment requires an effective management and monitoring of key risk domains. Depending on the relevance, each of these domain would help strengthen security and controls in your RPA environment.

RPA Specific Risk Considerations

Business Risk

• Alignment with organizational business continuity strategy and priorities
• Crisis mitigation planning
• Business continuity during process outages
• Disaster Recovery Strategy implementation planning

• Server security configurations
• Network Vulnerabilities
• Logical security controls
• Penetration testing
• Code Reviews

Cyber Security

Incident Management and Business Continuity

• Regulatory compliance reporting requirements
• Mandatory controls/ validation in solution
• Document/ change management controls
• Data lineage and traceability

Regulatory Compliance

• Ensuring protection of data across the RPA ecosystem
• Consent record and validity
• Private data identification
• Cross border data transfers

Data leakage and Privacy

Identity and access management

• Access Security strategy for and by BOT
• Segregation of Duties and sensitive access
• BOT IAM risks and measures

• Current Software License contracts lack clarity to allow BOT access to target application
• Penalties due to non compliance – Indirect usage

License Compliance

Secured Business process

• Weaker process / sox controls
• Possible manual override on BOT automation
• Weak change management process of BOT configurations

Deloitte's Risk Framework for RPA

| Strategic | Technology | Financial | Operational | Regulatory |

Risk Management For the BOT

A holistic risk validation of the RPA is conducted from perspective all key domains of RPA risks. Deloitte's **Secured RPA implementations and advisory services** encompasses a wide range of process and compliance needs.
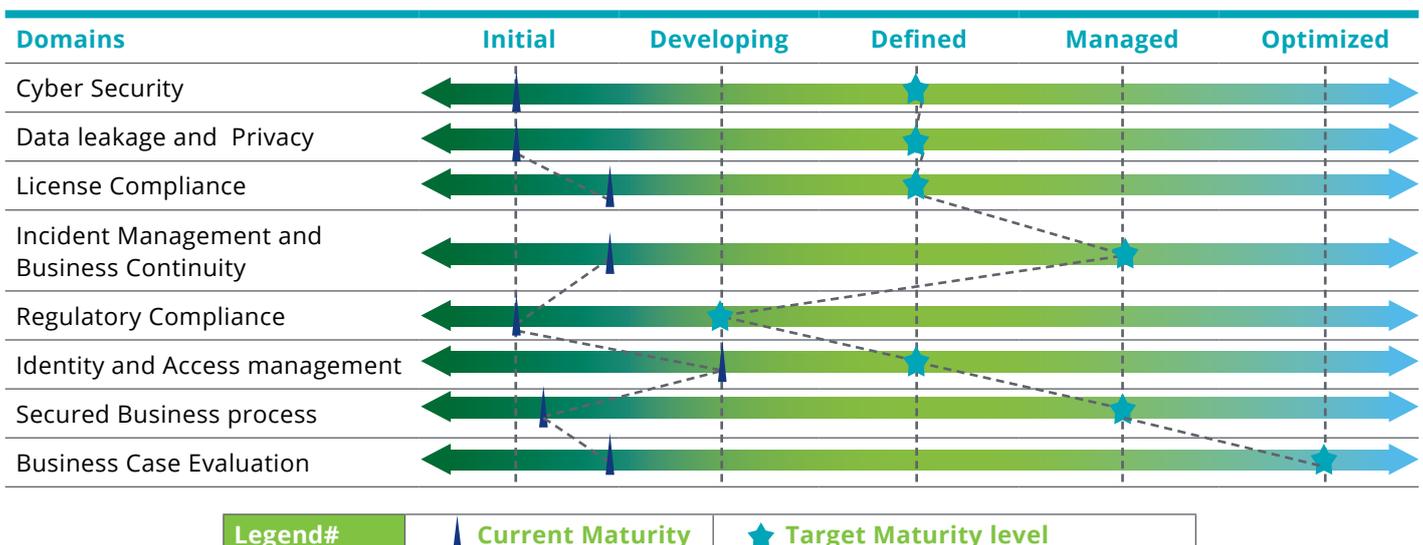
Implementation Advisory	**Secured BOT Assurance**	**Risk Management / Industry Solution**	**Managed Services**
BOT Security Architecture – Strategy, design and review	Secured BOT Assurance	Compliance enablers (SoX, JSOX, FRC, IFC, IRDA, TRAI, GST, ISO27001, PCI DSS etc.)	Governance Strategy
Identity and access management	Process and Access Control Design and implementation	Business Risk	Center of Excellence - Managed Cyber security operations center
Pre/ Post Go-live risk assessment	Functional and non functional Testing	Internal controls Monitoring	Incident management and response
Business Continuity Review	Vulnerability Management	Periodic Risk Assessment	Change Management validation
Process standardization and Mapping	Secured code reviews	Application License Compliance	IT Process Automation
Program governance and strategy	Interface / API Security	Industry solutions	Standard Operating Procedures
	Vulnerability Assessment	CSA Framework	Controls Automation

Our **Secured RPA implementations and advisory services** are designed to help you at varied stages of RPA implementation. It helps you get a comprehensive view of your RPA risks, maturity of risk management methods adopted along with desired state.

Typical value delivered includes:
- Independent and comprehensive BOT risk assessment
- Adoption of leading practices for secured and compliant BOT
- Assess the current RPA Risk maturity level and desired state
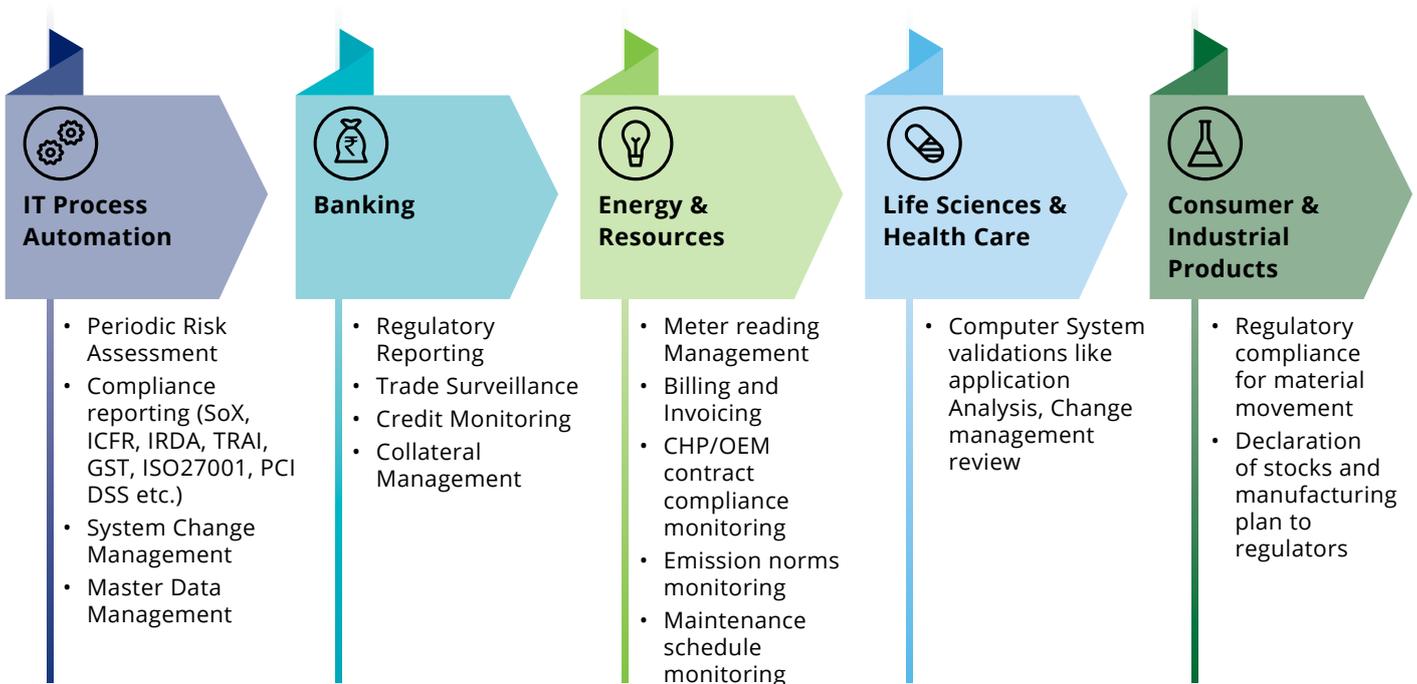
Illustrative   RPA Risk Maturity Benchmarking

Domains	Initial	Developing	Defined	Managed	Optimized
Cyber Security			★		
Data leakage and Privacy			★		
License Compliance			★		
Incident Management and Business Continuity				★	
Regulatory Compliance		★			
Identity and Access management			★		
Secured Business process				★	
Business Case Evaluation					★

Legend#	▮ Current Maturity	★ Target Maturity level

Risk Management By the BOT

Industries today face a large number of internal and external compliance requirements. With the regulators adopting technology, the demand for timely and granular compliance is common. RPA provide a unique value proposition for many such requirements. A carefully designed RPA can improve the accuracy of records and response time. On the other hand, with 100% review of records, compliance monitoring through RPA improves the quality of reviews and enhance stakeholder confidence.

Illustrative view of RPA amenable Risk Management use cases are highlighted below.

IT Process Automation

- Periodic Risk Assessment
- Compliance reporting (SoX, ICFR, IRDA, TRAI, GST, ISO27001, PCI DSS etc.)
- System Change Management
- Master Data Management

Banking

- Regulatory Reporting
- Trade Surveillance
- Credit Monitoring
- Collateral Management

Energy & Resources

- Meter reading Management
- Billing and Invoicing
- CHP/OEM contract compliance monitoring
- Emission norms monitoring
- Maintenance schedule monitoring

Life Sciences & Health Care

- Computer System validations like application Analysis, Change management review

Consumer & Industrial Products

- Regulatory compliance for material movement
- Declaration of stocks and manufacturing plan to regulators

How can we help?

Our RPA methodology is designed to help you throughout the RPA journey. Our team of risk and technology experts would help automate compliances as well secure your RPA environment.

Leveraging RPA for secured and compliant Technology environment
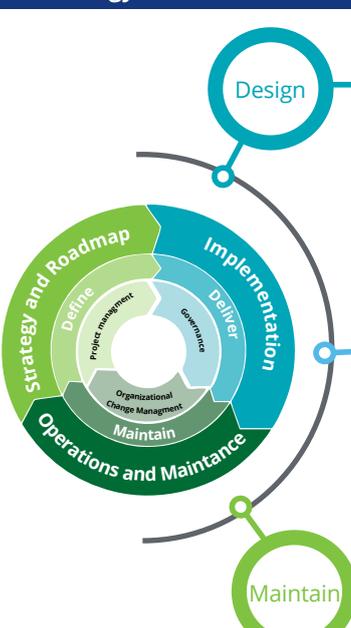
Its all in design. We bring our experience for enabling compliance across industries to help you choose the right candidates and design to-be processes. Maximum risk mitigation with optimal efforts.

Embedded controls is the best way to manage risks in any technology implementation. Our combined teams of technology and risk experts helps implement a secure RPA environment

With ever evolving risk and threats to the technology environments our experts help you prevent, detect and manage risks and threats to RPA environment

Design

Deploy

Maintain

Strategy and Roadmap
Define
Project management
Implementation
Governance
Deliver
Organizational Change Managment
Maintain
Operations and Maintance

Making your RPA environment secured and compliant

01 **Secured BOT Assurance for RPA implementation**

02 **Secured BOT Assurance for RPA products**

03 **RPA Risk Maturity Assessments**

04 **BOT Identify and Access Management**

05 **Managed Cyber security operations center – Center of Excellence**

06 **Incident management and response**
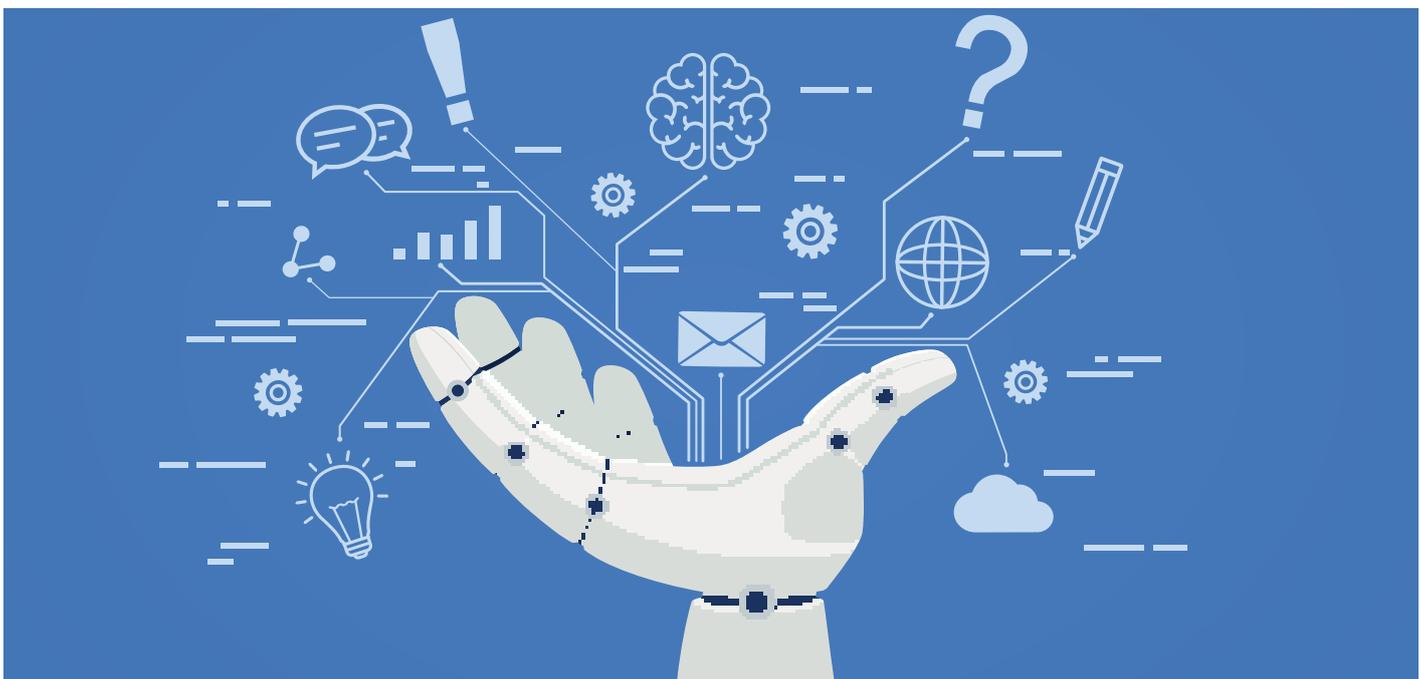
Contacts

Rohit Mahajan
President
Risk Advisory
E-mail: rmahajan@deloitte.com

Abhay Gupte
Partner
Risk Advisory
E-mail: agupte@deloitte.com

Ashish Sharma
Partner
Risk Advisory
E-mail: sashish@deloitte.com

Gaurav Shukla
Partner
Risk Advisory
E-mail: shuklagaurav@deloitte.com

Prasad Godbole
Senior Manager
Risk Advisory
E-mail: prasadsg@deloitte.com

Anthony Crasto
Partner
Risk Advisory
E-mail: acrasto@deloitte.com

Deloitte.