



BOT Identity Management

Secured BOT Series

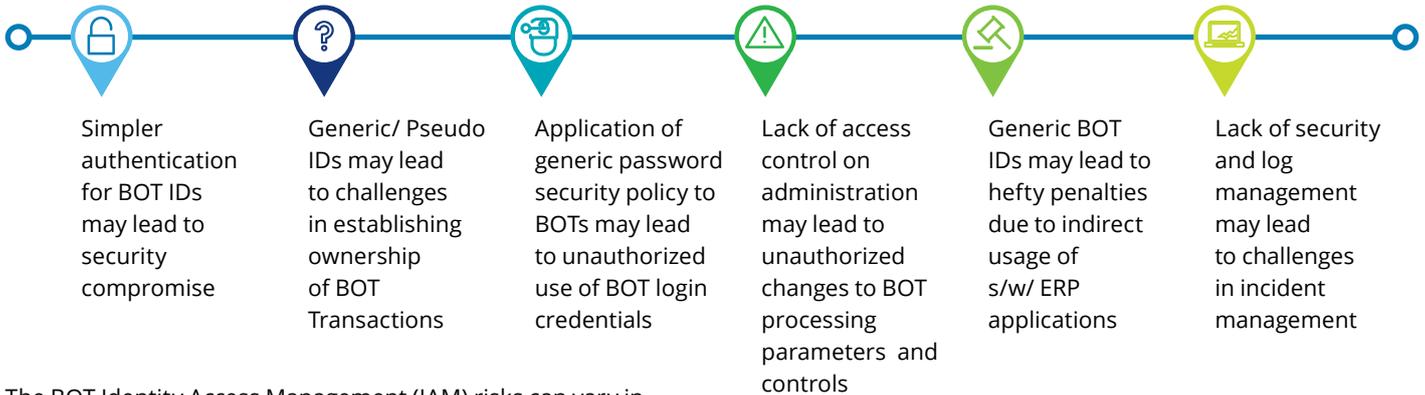
2019

BOT Identity: Secured. Optimized. Simplified.

Ro(BOT)tic Process Automation (RPA) has emerged as an enabler of efficient and error-free operations. The technology is designed to enhance productivity, and its agility enables quicker processing of multi-application data and efficient management of internal/external system access. Incidentally, it also opens doors to related cyber threats.



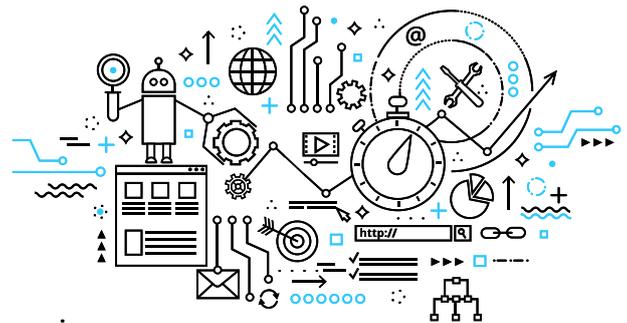
Key risks to BOT Identity Management:



The BOT Identity Access Management (IAM) risks can vary in complexity, size of application environment and number of BOTs

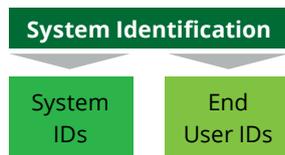
RPA IAM over Traditional IAM

Deploying traditional IAM needs user and system IDs to be segregated (based on nature of access and transactions handled). However, RPA (BOT) IDs are system IDs and access applications like humans.

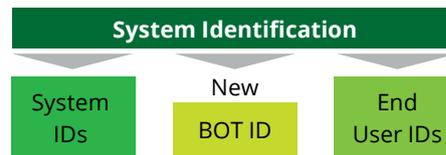


We understand the challenges of IAM deployment in a BOT environment.

Traditional Scenarios



RPA scenarios

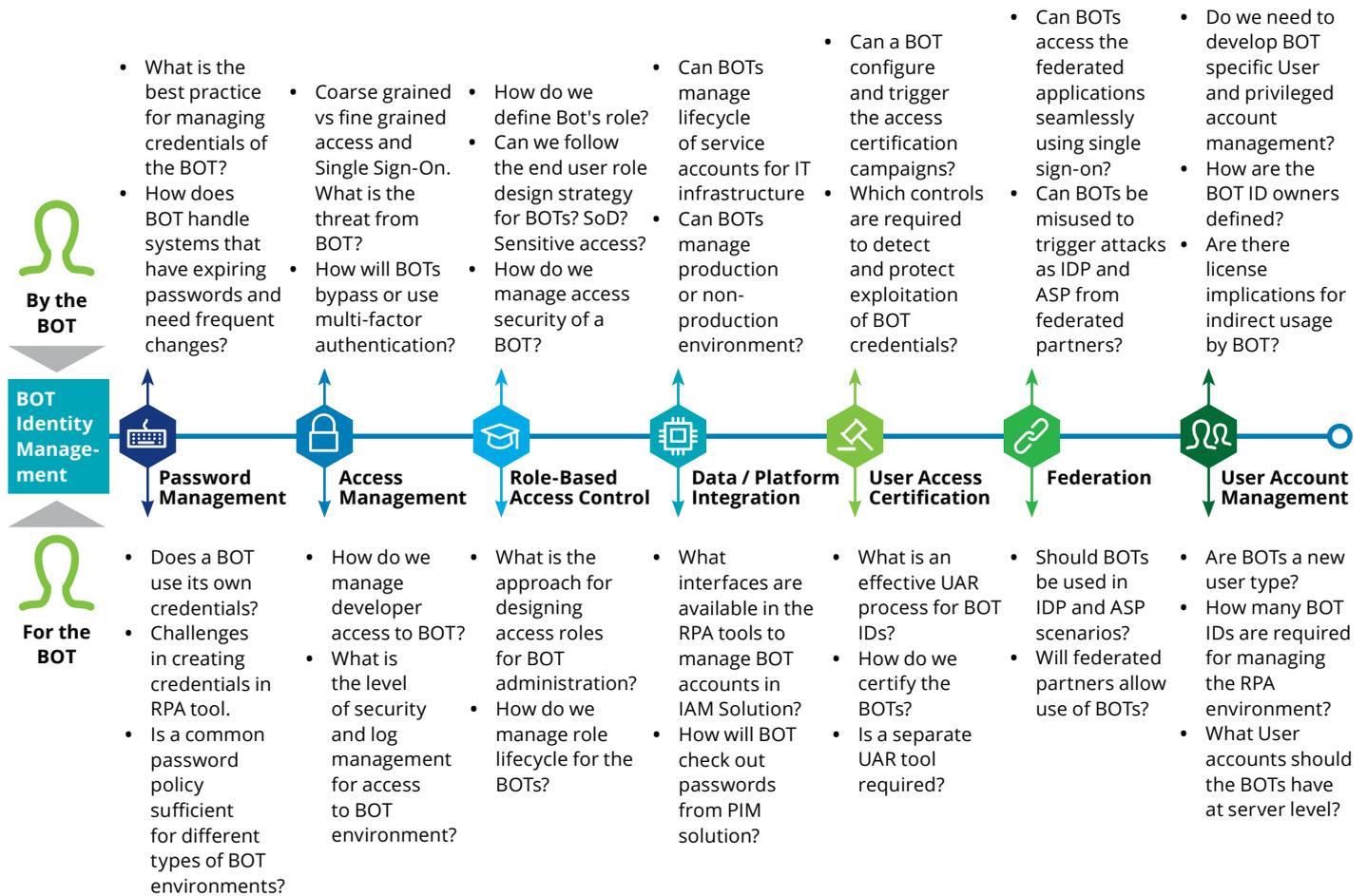


Access systems like Humans but operate as System IDs

Authentication	Single Sign on	One factor Single Sign-on is too risky. Consider API based just in time tokens or other mechanism for second factor. Special considerations for cases where biometrics for human interaction are mandated.
SOD	Segregation required to avoid conflict of interest	BOTs would not have conflicting interests; however, two BOTs with SOD violation cannot be owned by one human.
Fire Fighter	BCM requirement, robust monitoring	Traditional fire fighting principles may not apply to organisations with 24x7 BOT world
License Compliance	As per pre defined License contract terms	BOTs have direct implications on indirect usage. Non-human interaction with applications can void OEM warranty or violate terms of agreement.
Audit trail	Required for traceability	Redefine the purpose of Audit trail. Risk gets reformed with RPA and requires additional monitoring of BOT activity by SIEM systems
# ID	One is to one ratio, with business roles	One ID to many BOTs? Or One ID per BOT? Both options have pros and cons and a collective assessment of above parameters would lead to the best choice.

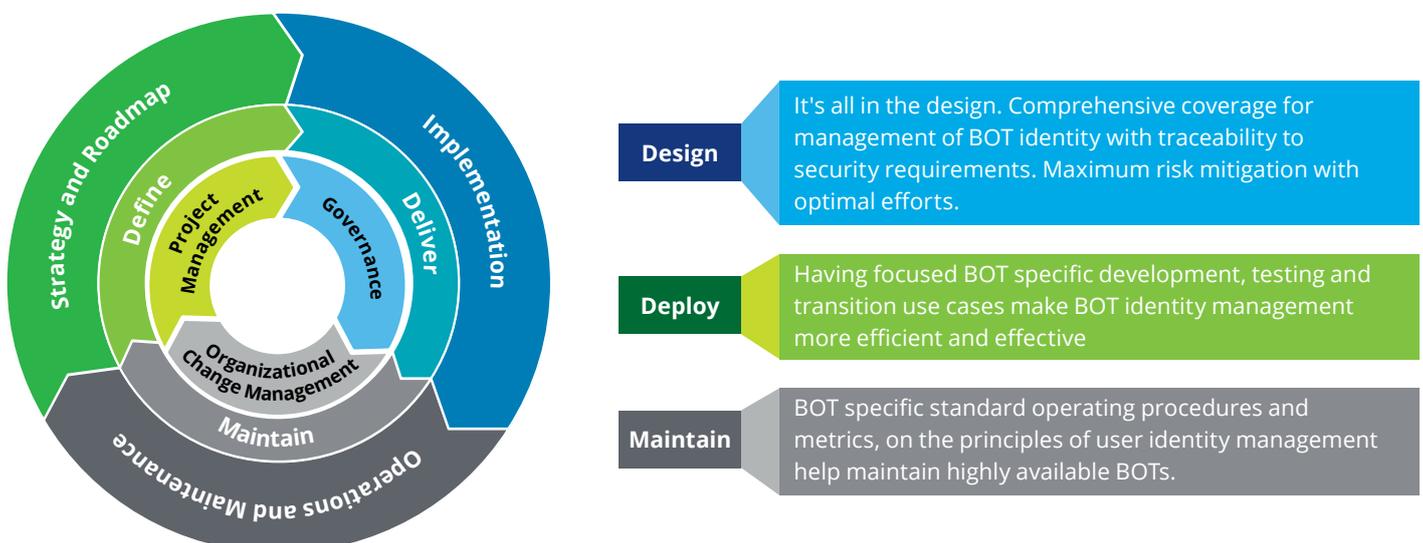
How do we look at IAM for the BOT world?

Identity Management for BOTs needs to be addressed from two perspectives, "For The BOT" and "By The BOT". We, at Deloitte, leverage our IAM Methods® to address RPA specific challenges. The seven components of Deloitte IAM Framework are further elaborated to address RPA risks and remediation requirements.



How can we help?

Deloitte's RPA IAM methodology is designed to help you throughout the RPA journey. Our team of IAM experts would help secure the identity management 'of' and 'by' the BOT.



Service Catalogue – Governance, Risk and Compliance solutions for RPA

Implementation Advisory	Secured BOT Assurance	Risk Management / Industry Solution	Managed Services
<ul style="list-style-type: none"> • BOT Security Architecture – Strategy, Design and Review • Identity and Access Management • Pre/ Post Go-live Risk Assessment • Business Continuity Review • Process Standardization and Mapping • Program Governance and Strategy 	<ul style="list-style-type: none"> • Secured BOT Assurance • Process and Access Control Design and Implementation • Functional and Non-Functional Testing • Secured Code Reviews • Interface / API Security • Vulnerability Assessment 	<ul style="list-style-type: none"> • Compliance enablers (SoX, ICFR, IRDIA, TRAS, GST, ISO27001, PCI DSS etc.) • Internal Controls Monitoring • Periodic Risk Assessment • Regulatory Reporting • Application License Compliance • Industry Solutions 	<ul style="list-style-type: none"> • Governance Strategy • Center of Excellence • Managed Cyber Security Operations Center • Incident Management • Change Management • IT Process Automation

Contacts

Rohit Mahajan
 President
 Risk Advisory
rmahajan@deloitte.com

Gaurav Shukla
 Partner
shuklagaurav@deloitte.com

Ashish Sharma
 Partner
sashish@deloitte.com

Prasad Godbole
 Director
prasadsg@deloitte.com



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.