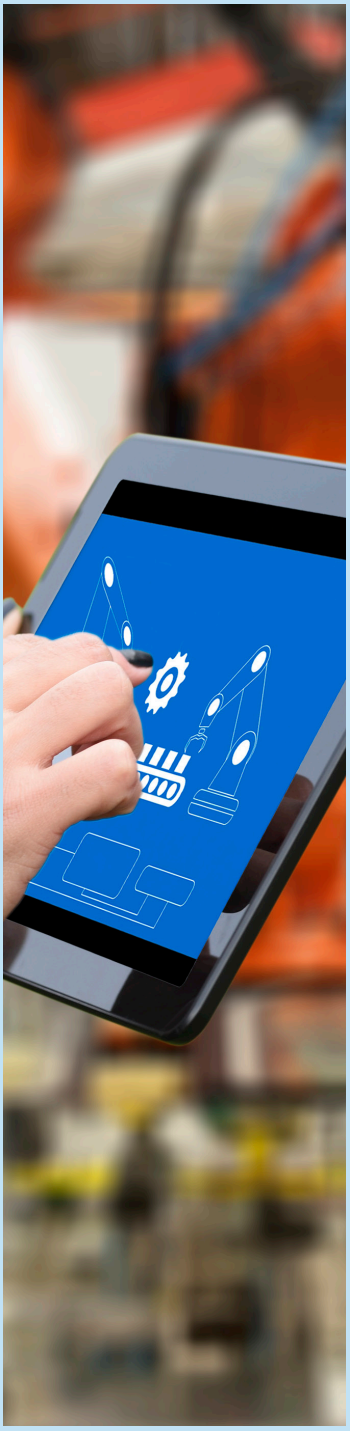
VIEW POINT



# SECURITY CONSIDERATIONS IN ROBOTIC PROCESS AUTOMATION


## Abstract

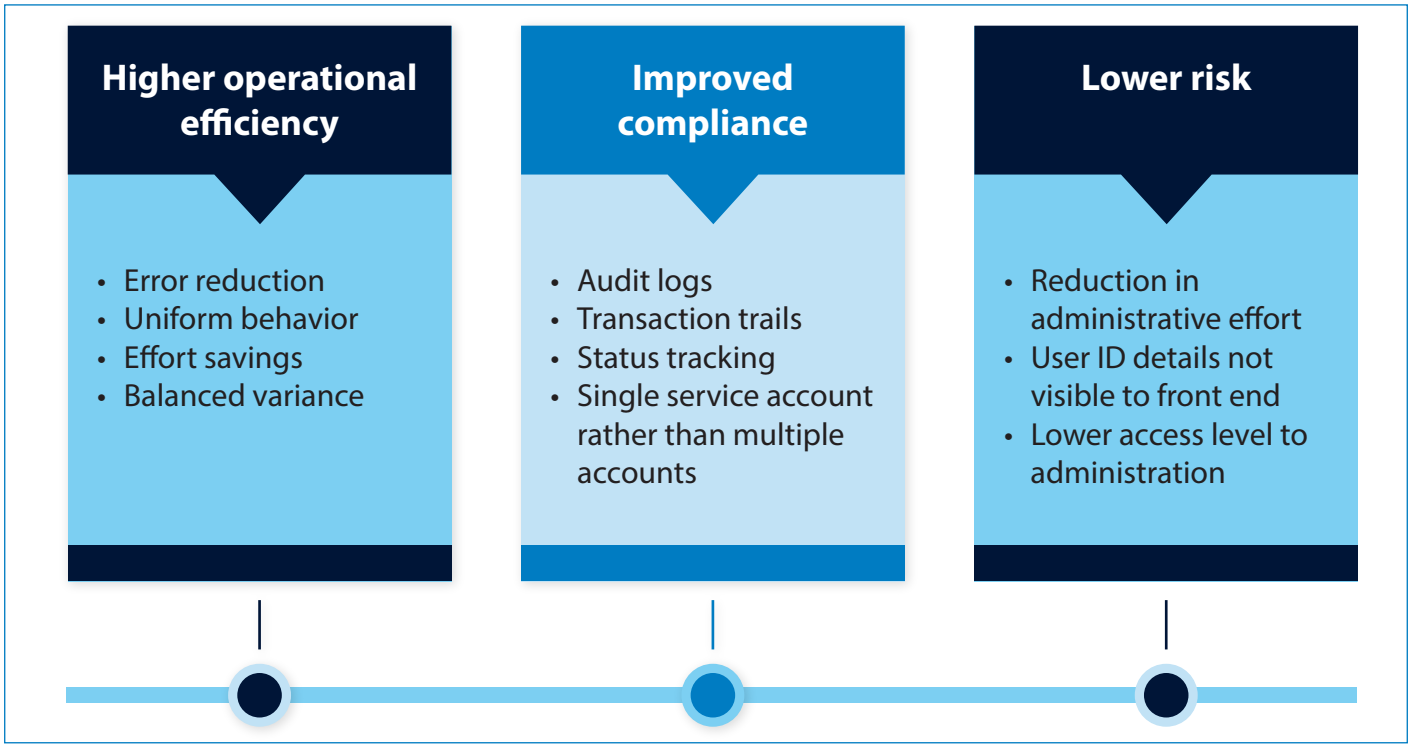
Robotic process automation (RPA) is delivering greater process efficiency, accuracy and integrity, helping organizations slash cost and effort while boosting productivity. However, in its current state, there are limitations to how much RPA software can mimic human actions, particularly when it comes to security and handling sensitive data. This paper examines how RPA may increase the risk exposure for organizations. It also discusses some key considerations to ensure enterprise and data security when adopting RPA.


Infosys®
Navigate your next

## The value of RPA

Over the past few years, robotic process automation (RPA) has become a popular technology due to its ability to automate repetitive and high-volume tasks in order to reduce manual effort, eliminate error and improve process productivity. With RPA, software bots can mimic human actions such as logging into various applications/systems and navigating through user interfaces to perform tasks such as creating tickets and downloading data. Bots can also provision and deprovision user access and respond to customer queries.

RPA is versatile and flexible, allowing it to integrate easily with existing processes. It helps reduce cost, maintain consistent quality, improve delivery timelines, and enhance the customer experience.

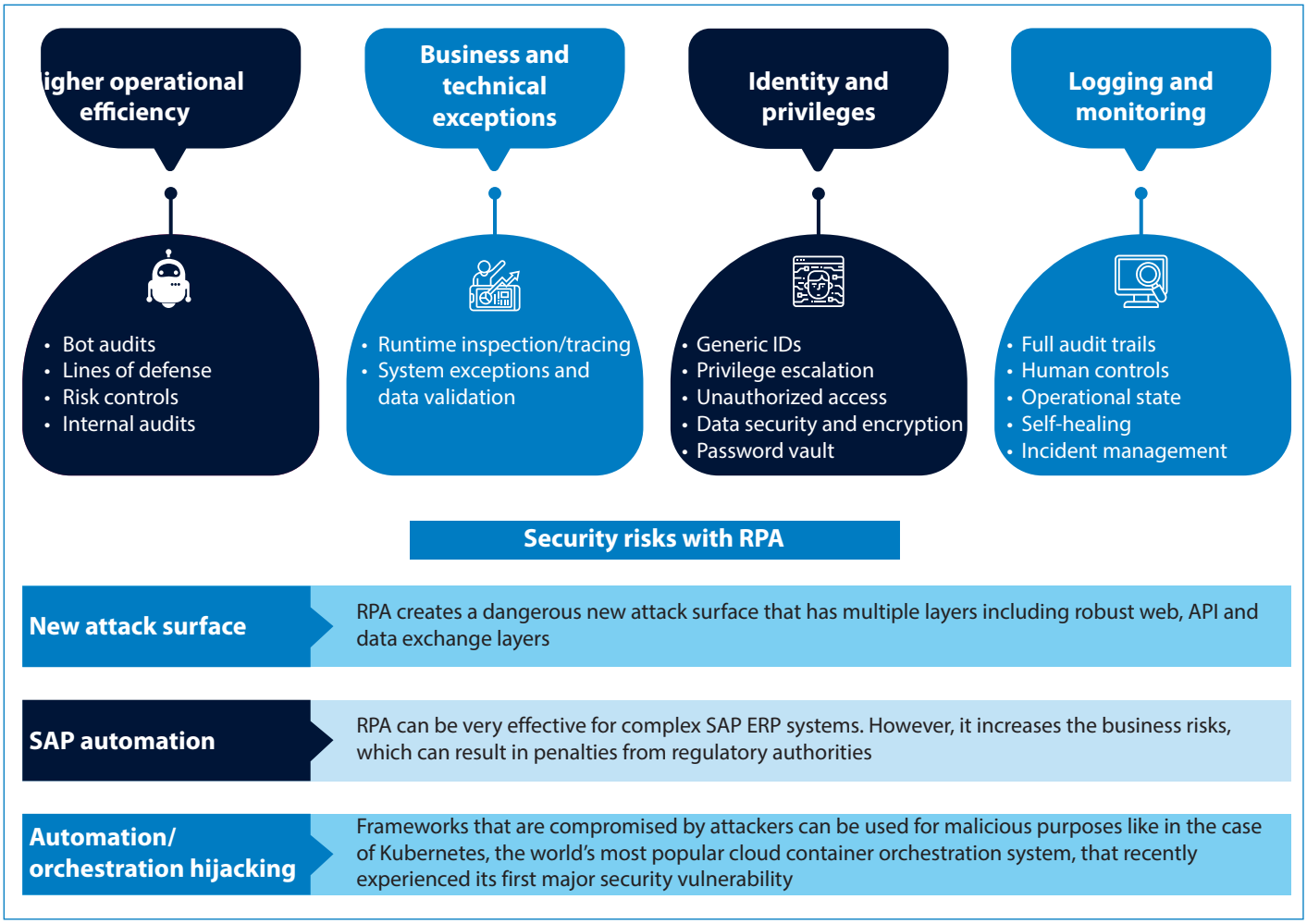



## Security challenges with RPA

Organizations looking to implement RPA should be aware of the security-related challenges. These include:

- **Need to maintain audit logs** – Audit logs capture bot activity. These are important to track bot health and effectiveness. For instance, if a bot stops working, the audit log helps identify the underlying reason, whether it is improper use by an employee or malicious code
- **Lack of bot password management** – In the case of human users, passwords are confidential and can be reset regularly to prevent unauthorized access. However, this cannot be implemented for bots due to the lack of proper tools
- **Need for constant supervision** – Bots need to be periodically monitored at various levels to ensure they do not misbehave, which can lead to high error rates and potential damage
- **Ineffective bots** – In some cases, bots may not perform as intended due to erroneous coding or inadequate testing. This will result in issues and errors during go-live
- **Data misuse** – For some processes like payroll management and file transfer, bots require access to private information such as passwords, addresses, credit card numbers, etc., of employees, clients and vendors. The challenge here is ensuring that corporate as well as personal data remains confidential and is not misused

## Security risks with RPA




- **Higher risk exposure** – The automation involved in RPA creates several layers such as the web, APIs and data exchange that are vulnerable to attacks
- **Unsecure frameworks** – The use of RPA frameworks can expose organizations to new types of cyber-threats
- **Costs of non-compliance** – Implementing RPA may increase business risk, leading to steep fines imposed by regulatory bodies for non-compliance or security breaches

In the hands of malicious users, RPA bots can be developed to breach an organization's defenses and steal confidential data. Bots can be used to track the product listings of competitors, which constitutes data theft. They can be programmed to steal content to outrank authentic results on a search engine's pages. For organizations that have invested significantly in developing original content for their websites, such attacks can devalue their web presence and even lead to revenue loss. Bots can also be used to spam community forums with invasive advertisements and create wrongful impressions on mobile applications through fake advertisements.

## Mitigating security risk in RPA

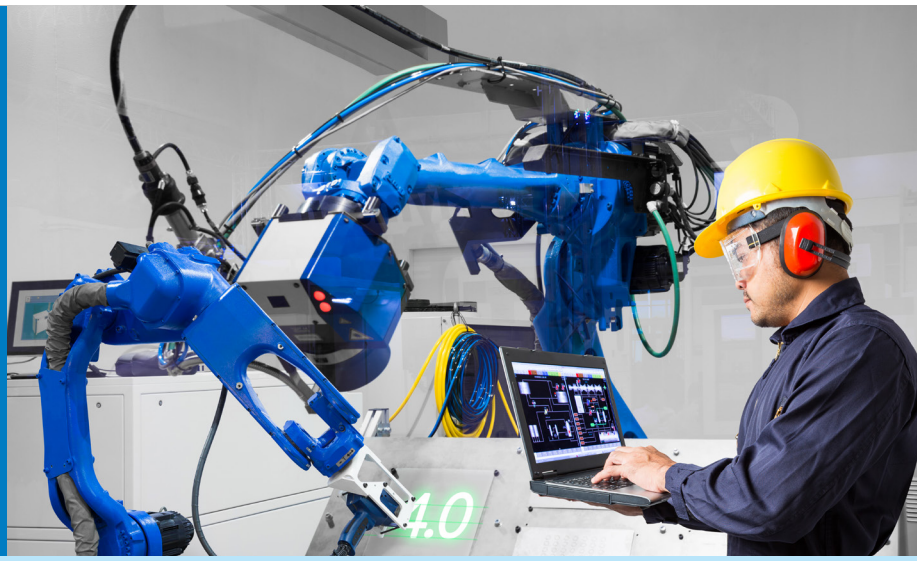
- **Conduct regular audits and periodic risk assessments** – Implement proper controls to monitor RPA activities and ensure that all bots are operating within the defined set of rules. This RPA log should be reviewed regularly. Periodic risk assessment is also needed to track the emergence of new risks, check whether controls have lapsed and determine whether any robot should be retired
- **Control access to the RPA environment** – Organizations should be careful about how they grant access to analysts that work in RPA environments. For instance, personal IDs should never be used in RPA; instead it is preferable to use generic IDs
- **Follow strict governance** – Rules and controls must be defined clearly to ensure RPA security. The governance framework should include detailed standards, business justification and development standards

- **Use a password vault** – Password vaults allow RPA teams to store all the passwords in a single repository without compromising security
- **Choose the right RPA candidates** – Organizations should leverage a best practice based assessment approach to identify the right candidates for RPA. For instance, the assessment approach should delineate the current risks and complexity within the existing processes
- **Implement robust change management** – A structured change management process is crucial to ensure accountability and auditing of RPA implementation. This should define who is responsible for executing changes, assessing risk, reviewing performance, providing approvals, running back-ups of prior versions, and sending notifications to the user community
- **Ensure process continuity** – A clear business continuity plan must be created that outlines the back-up procedures and information sources needed to perform each task. An internal audit team should check whether the business continuity plan documents have the details such as how each process/activity will be resumed in case of failure.

Apart from the above steps, organizations should ensure that bots comply with the organization's standards and security controls. To this end, bot monitoring and error handling should be automated steps so that malware is identified and remediated early on. The code created by RPA developers should be reviewed thoroughly to prevent breaches or errors. Finally, all bot activities and changes should be versioned and validated to provide an audit trail for compliance.

## Conclusion

Organizations adopting RPA to improve productivity should plan their implementations carefully to protect themselves from security breaches. RPA creates new application layers that are vulnerable to risk. Moreover, without constant supervision, bots may fail to work effectively, causing issues, errors and potential damage. Since bots may need access to private information, it is imperative for organizations to institute the right security measures. Some of these measures include creating governance frameworks, audit logs, password vaults, and version controls. Establishing these processes will allow RPA to handle security risks by itself, thereby ensuring optimal bot performance and reduced business risk.




## About the Author

**Kanchana** comes with over 10 years of IT experience in the IDAM, Auditing and Automation domain. In addition to these, Kanchana has been a subject matter expert in the UAM projects. She has also been involved in project recovery, transition and few of the presales activities, and internal audits. In the current role, Kanchana is responsible for automation rollouts in projects across cybersecurity towers and standardization initiatives.

For more information, contact askus@infosys.com

Infosys®
Navigate your next