Deloitte.

Auditing the RPA environment

Our approach towards addressing risks in a BOT environment

March 2018

Automation is the buzzword today and companies of various sizes are implementing Robotic Process Automation (also referred to as RPA or BOT) in various business processes. The benefits such as controls effectiveness, process efficiencies, and improved customer experiences have enticed organizations to adopt different levels of automation in their businesses.

There are multiple aspects of process automation which lead to an elevated risk exposure as compared to a typical IT Application. To name a few from an audit perspective, there are changes in process risk definitions post automation, changes to job roles and access security, application change management considerations, strategy and governance of RPA environment, etc.
Changing the control design post automation is one of the most ignored areas in the need for speed of implementation. Automation of a business process results in changes to process control requirements. This makes it critical for auditors to audit these automated environments to have a comfort over the output from the BOT. The auditor sometimes looks out for strong input-output controls for having a reasonable assurance over the BOTs.

This PoV highlights the different factors involved in auditing the RPA enabled environment. As the RPA is still evolving, there are no standards specifically available for auditing the RPA environments (except for some in the production area). In most cases of RPA implementation, the focus is on reducing cost in minimum possible time and hence, not much emphasis is placed on compliance to policies and procedures with respect to creation and maintenance of BOTs.

There are certain procedures we perform at various stages in the audit lifecycle to address the specific risks emerging from of an automated setup. The following table illustrates the various phases of audit and the key considerations that the Management and the Auditors need to take care of:

1. In the planning phase, a clear understanding is to be obtained about the areas where the BOT is implemented. It is also important to understand the level of robotic process automation: Partial, Complete, or No automation in the planning phase to be better prepared for the audit. The Deloitte risk management framework helps to get the risk assessment completed with accuracy.

2. Once the auditor identifies that there are automations in an environment, a specialist with the required skillsets needs to be included in the team upfront, right from the walkthrough stage. It is important to identify the additional system to test the risks associated with each automation in the processes.

3. BOTs need to be considered as elements of the IT. Not every BOT becomes relevant for audit; due care has to be taken by the auditor to scope-in the BOTs specifically relevant for our testing. If there are some controls performed by the BOTs such as generating reports that are used by the auditor or by the management, it needs to be scoped-in for our general control reviews.

4. Previously, the auditors used to perform a walkthrough of the process which would help them understand risks, controls, systems involved, interfaces etc. However, in the case of a walkthrough of a BOT environments, a code walkthrough becomes critical as well. Scoping of IPE/IUC would also need a separate thought process.

5. The auditor needs to evaluate whether there are any exception reports which come out of the BOT which are either reviewed by the management or used by the auditor for performing their audit procedures. If there are such reports, the auditor needs to assess the completeness and accuracy of such information by evaluating the source code, logic and the parameters.

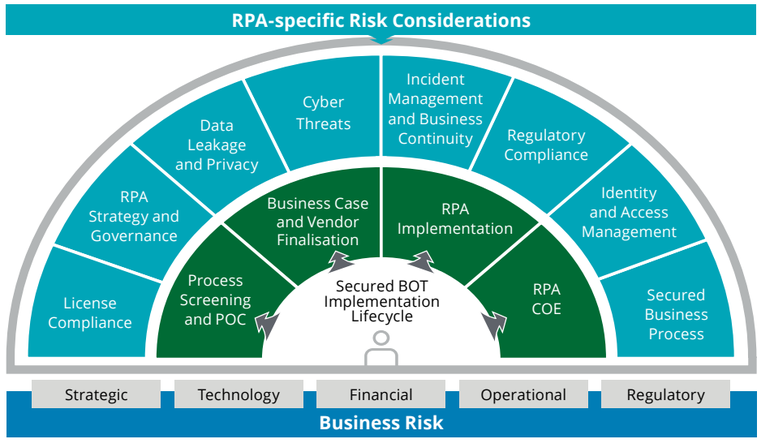
6. Also, there can be interfaces between various BOTs. It is important to audit the relevant interfaces. The auditor will need to understand whether these interfaces are unidirectional or bidirectional before testing how they are configured to ensure completeness and accuracy.

Considerations at different phases of audit when auditing a BOT environment

Phases of Audit		Considerations
Planning	• Detailed understanding of the areas where RPA is implemented • Audit Plans	• Audit plans and risk assessment for RPA • Update to control matrices for automation through RPA • Upfront involvement of IS Auditor/BOT Specialists
Walkthrough	• Understanding of the process & IT • Identification of Risks • Identification of Controls	• New IS/IT risks and scoped in systems • Changes to automated controls, IPE/IUC , audit logs and interfaces • More IS Risks and therefore enhanced ITGCC controls
Design Evaluation	• Evaluation of the Design of controls • Exception handling process • Identification of gaps	• Substantial work by IS Auditor to test controls from Design (Configuration controls, logs, Cyber risks) • Testing for IPE/IUC
Operating effectiveness	• Controls Testing • Substantive Testing	• Increased controls testing and minimal substantive testing • Process governance and roles
Reporting	• Gaps reporting • Recommendations	• Logs and audit trails • Changes to control design, RCM, SOPs, roles etc. • Technology recommendations

Introduction to the Deloitte risk management framework for RPA
RPA brings its own inherent risks as well as those which are resultant of the technology environment it automates. A secured and compliant BOT environment requires effective management and monitoring of the seven risk domains. Depending on the relevance, each of these domains would help strengthen security and controls in your RPA environment.

The adjacent framework presents a clear view about the types of risk which need to be considered when auditing a BOT-enabled organization. The auditor should try to use a risk based approach to identify the controls addressing each of the RPA-specific risk consideration.



Every domain of general IT controls such as user-access management, change management, operations, and program development is important to be looked at for the relevant BOTs. Following would be some of the probing questions to understand the controls in a BOT environment:

License Compliance
- Have you taken care of software license compliance post automation?

RPA Strategy and Governance
- Have you involved Internal/ External Auditors or compliance teams as part of your governance committee?
- Have you considered an impact of RPA on the following?
  - Control matrices or monitoring mechanisms
  - Standard operation procedures
- Have you assessed changes to roles and responsibilities post RPA?

Data Leakage and Privacy
- How do you ensure accuracy, security and completeness of the stored data?

Cyber Threats
- Is there an associated cyber-risk and how is it controlled? Does your vulnerability management program cover the BOT landscape?

Incident Management
- How are the incidents remediated in the RPA environment?
- Do you have log monitoring for all critical actions to and by the BOT?

Business Continuity
- Have you ensured a defined IT disaster recovery and scalability plan?
- Do you perform regular testing to assess the failover and recovery capability and plans to ensure any disruption in the robotic availability does not impact the business operations?
- Do you have a fall-back plan for a situation when the human workforce no longer knows the manual steps that were previously undertaken?

Regulatory Compliance
- What procedures are followed for Change management? Are they documented?
- Are BOT security and protection requirements
- What is the mechanism in place for data lineage and traceability?

Identity and Access Management
- How are the privilege accounts for RPA environment controlled? IDs and the end users?
- Whether access is appropriately segregated between BOT
- Are passwords encrypted, stored and set as per policies and procedures?

Secured Business Process
- Have you assessed changes to automated/ manual controls environment due to RPA implementation? How do you ensure processing errors are corrected to successful completion/ posting?
- Are critical systems, programs, and/or jobs monitored?
- Do you have change management process for the RPA environment?

Conclusion

It is evident that auditing an RPA environment is quite different from conventional audits and that auditors have to upskill themselves to audit such complex environments. We will not have to wait for long to see a BOT reviewing another BOT and providing exception reports which go to a human reviewer.

The audit approach will move towards testing more preventive controls and we will see more of exceptions-based testing rather than sample-based/ transaction-based audits.

Contacts

Anthony Crasto
President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Abhijit Katkar
Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Kamaljit Chawla
Leader – Cyber Operate
Risk Advisory, Deloitte India
kamaljitc@deloitte.com

Tarun Kaura
Leader - Cyber Advisory
Risk Advisory, Deloitte India
tkaura@deloitte.com

Deepa Seshadri
Partner, Risk Advisory
Deloitte India
deseshadri@deloitte.com

Ashish Sharma
Partner, Risk Advisory
Deloitte India
sashish@deloitte.com

Deloitte.