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, operational and regulatory.

Process risk definitions post automation, IT Application. To name a few from an operational view, the Auditors need to take care of:

- BOTs in various business processes. The auditor needs to assess the risks associated with each automation in the processes.
- Considerations at different phases of audit when auditing a BOT environment
- 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.
- Also, there can be interfaces between various BOTs. It is important to audit the relevant interfaces. The auditor needs to understand whether these interfaces are unidirectional or bidirectional before testing how they are configured to ensure completeness and accuracy.
- 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.

Introduction to the Deloitte risk management framework

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:

- Are BOT security and protection requirements documented?
- What is the mechanism in place for data lineage and traceability?
- Are passwords encrypted, stored and set as per policies and procedures?
- How do you ensure processing errors are corrected to prevent further issues?

Considerations at different phases of audit when auditing a BOT environment

**Phases of Audit**
- Planning
  - Detailed understanding of the areas where RPA is implemented
  - Audit Plans
- Walkthrough
  - Understanding of the process & IT Environment
  - Identification of Risks
  - Identification of Controls
- Design Evaluation
  - Evaluation of the Design of controls
    - Exception handling process
    - Identification of gaps
- Operating effectiveness
  - Controls Testing
    - Testing for IPE/IUC
  - Gaps reporting
    - Recommendations
- Reporting
  - Logs and audit trails
  - Changes to control design, RCM, SOPs, roles etc.
  - Technology recommendations

<table>
<thead>
<tr>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit plans and risk assessment for RPA</td>
</tr>
<tr>
<td>Update to control matrices as and when through RPA</td>
</tr>
<tr>
<td>Upright involvement of IS Auditor/BOT Specialists</td>
</tr>
<tr>
<td>New IS/IT risks and scoped in systems</td>
</tr>
<tr>
<td>Changes to automated controls, IPE/IUC, audit logs and interfaces</td>
</tr>
<tr>
<td>More IS Risks and therefore enhanced ITGRC controls</td>
</tr>
<tr>
<td>Substantial work by IS Auditor/BOT specialists</td>
</tr>
<tr>
<td>How are the incident remediated in the RPA environment?</td>
</tr>
<tr>
<td>Have you assessed changes to roles and responsibilities post RPA?</td>
</tr>
<tr>
<td>Have you assessed changes to procedures for Change management?</td>
</tr>
<tr>
<td>Are BOT security and protection requirements documented?</td>
</tr>
<tr>
<td>Are passwords encrypted, stored and set as per policies and procedures?</td>
</tr>
<tr>
<td>How do you ensure processing errors are corrected to prevent further issues?</td>
</tr>
<tr>
<td>What is the mechanism in place for data lineage and traceability?</td>
</tr>
<tr>
<td>Are controls segregated between BOTs?</td>
</tr>
<tr>
<td>How do you ensure processing errors are corrected to prevent further issues?</td>
</tr>
<tr>
<td>How do you ensure processing errors are corrected to prevent further issues?</td>
</tr>
</tbody>
</table>

**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.
Contact

Deepta Seshadri
Partner – Risk Advisory
deseshadri@deloitte.com

Ashish Sharma
Partner – Risk Advisory
sashish@deloitte.com