# Technology Impact and Changing Dynamics of Internal Audit

Posted Feb 26, 2021

Bharat Shah

**Associate Director, RSM India**

Anup Nair

**Director-IT Systems Assurance, RSM India**

## Introduction

The Digital and Mobility revolution has improved, impacted as well as disrupted businesses, business models, processes, etc. The emergence of as e-commerce, mobile applications, sophisticated ERPs, block chain solutions, cloud computing, robotic Business Process Automation

(RPA), Internet of Things (IoT), Machine Learning (ML) and Artificial Intelligence (AI) have added new dimensions to businesses. The internal audit function needs to re-orient itself to meet the requirements in this Digital Era as well as improve its own approach and methodology to be relevant and effective.

**Some of the key questions around Information Technology (IT) risk management and Internal Audit**

Are the controls and Segregation of Duties (SoDs) mapped correctly in your IT/ERP systems? What are the over-rides and the mechanisms for audit trails of such over-rides?

Does your audit plan identify key IT risks that have direct significant impact on the organisation?

Is IT audit part of your internal audit plan?

Have you identified opportunities to reduce manual controls by increasing automated controls?

Have you identified areas in your internal audit plan where data analytics can be used for the audit of complete or larger set of data set rather than sample based approach?

Have you assessed the business, financial, legal and reputational risks associated with data leakage or cyber frauds? Have you effective control and audit mechanisms in place to counter the same?

Have you ascertained applicable data privacy regulations and put in place the mechanism required to conform to the same? Are the same covered in the internal audit and/or IT systems audit?

Have you identified the laws requiring digital filings and reporting? Are their effective controls for the digital authorization of the filings (DSCs), review of compliances, receipt and adherence to any on-line notices/proceedings, etc.?

Have you identified areas in your audit plan where technology can be used to evaluate the effectiveness of controls against the key risks?

Does your Internal Audit team have sufficient IT competencies to evaluate the effectiveness of controls?

Do you have a program/framework established to ensure the above aspects are verified on a continual basis?

**Information Technology in Internal Audit  A Key Differentiator**

Internal audits are designed to evaluate the effectiveness of organisations internal controls by first gathering information about how a unit operates, identifying points at which errors or inefficiencies are possible and identifying system controls designed to prevent or detect such occurrences. Then, the application and performance of those controls are tested to assess how well they work. Managers ought to routinely evaluate controls in their department's operations by following the same process.

IT provides most of the information needed for auditing. In order to be effective, auditors must use IT as an auditing tool, audit automated systems and data, to understand the business purposes for the systems, and understand the environment in which the systems operate.

The other important uses of IT by auditors are in audit administration. By seeking new use for computers and communications, auditors improve their ability to review systems and information and manage their activities more effectively. Automated tools allow auditors to increase individual productivity and that of the audit function. By recognising the importance of emerging environment

and requirement to perform audit task effectively, auditors must recognise the key reasons to use audit tools and software.

Some of the examples below demonstrate the need for an effective Internal Audit function leveraging technology platform.

**Key IT considerations for Internal Audit**

**Information Security**

| Information Security | Key IT Internal Audit Considerations |
| --- | --- |
| Information security program assessment – Evaluates theorganisation's information security program, includingstrategy, awareness and training, vulnerability assessments, predictive threat models, monitoring, detection and response, technologies and reporting. | How comprehensive is the existing information security program?<br>Is information security embedded within the organisation, or is it an "IT only" responsibility?<br>How well does the organisation self-assess threats and mitigate the threats?<br>How well the organisation find the vulnerabilities and the solution for that? |
| Threat and vulnerability management program assessment –Evaluates the organisation's Threat and VulnerabilityManagement (TVM) program including threat intelligence, vulnerability identification, remediation, detection, response, and countermeasure planning. | How comprehensive is the existing TVM program?<br>Is the TVM program aligned with business strategy and the risk appetite of the organisation?<br>Are the components of TVM integrated with one another, as well as with other security and IT functions?<br>Do processes exist to make sure identified issues are appropriately addressed and remediation is effective?<br>What counter measures have been planned for the threats with the TVM? |

**Business Continuity Management**

| Business Continuity Management | Key IT Internal Audit Considerations |
| --- | --- |

| | |
|---|---|
| Business continuity program integration and governance audit  Evaluates the organisations overall business continuity plan, including program governance, policies, risk assessments,business impact analysis, vendor/third-partyassessment, strategy/plan,testing, maintenance, change management and training/awareness | Does a holistic business continuity plan exist for the organisation?<br>How does the plan compare to leading practice?<br>Is the plan tested?<br>What impact the plan and how the plan will affect the business? |
| Disaster recovery audit  Assesses ITs ability to effectively recover systems and resume regular system performance in the event of a disruption or disaster. | Are disaster recovery plans aligned with broader business continuity plans?<br>Do testing efforts provide confidence systems that can be effectively recovered?<br>Are all critical systems included? Are critical systems defined? |
| Crisis management audit  Reviews the organisations crisis management plans, including overall strategy/plan, asset protection, employee safety, communication methods, public relations, testing, maintenance, change management and training/awareness. | Are crisis management plans aligned with broader business continuity plans?<br>Are plans comprehensive and do they involve the right corporate functions?<br>Are plans well communicated? |

**Mobile Security**

| | |
|---|---|
| Mobile Security<br>Mobile device configuration review  Identifies risks in mobile device settings and vulnerabilities in the current implementation. This audit would include an evaluation of trusted clients,supporting network architecture, policy implementation, management of lost or stolen devices, and vulnerabilityidentification through network accessibility and policy configuration. | Key IT Internal Audit Considerations<br>How has the organisation implemented bring your own device (BYOD)?<br>Are the right policies/mobile strategies in place?<br>Are mobile devices managed in a consistent manner?<br>Are configuration settings secure and enforced through policy?<br>How do we manage lost and stolen devices?<br>What vulnerabilities exist, and how do we manage them? |
| Mobile application black box assessment  Performs audit usingdifferent front-end testing strategies<br>scan for vulnerabilities using various tools, and manually verify scan results.<br>Attempts to exploit the vulnerabilities identified in mobile web apps. | What vulnerabilities can be successfully exploited?<br>How do we respond when exploited, and do we know an intrusion has occurred? |

| | |
|---|---|
| Mobile application grey box assessment  Combines traditional source code reviews (white box testing) with front-end (black box) testing techniques to identify critical areas of functionality and for symptoms of common poor coding practices.<br>Each of these hot spots in the code should be linked to the live instance of the application where manual exploit techniques can verifythe existence of a security vulnerability relations, testing, maintenance, change management and training/awareness. | How sound is the code associated with the mobile applications used within the organisation?<br>What vulnerabilities can be exploited within the code?<br>Whether OWASP top 10 vulnerabilities are present in the code? |
| Device Security configuration | Have your IT servers, infrastructure securely hardened?<br>Are the security patched updated appropriately?<br>Do you follow leading industry practices to secure systems? |

## Cloud Security

| | |
|---|---|
| Cloud Security<br>Cloud strategy and governance audit  Evaluates the organisations strategy for utilizing cloud technologies.<br>Determines whether the appropriate policies and controls have been developed to support the deployment of the strategy.<br>Evaluates alignment of the strategy to overall company objectives and the level of preparedness to adopt within the organisation. | Key IT Internal Audit Considerations<br>Are there supporting policies to follow when using a cloudprovider?<br>Are policies integrated with legal, procurement and IT policies?<br>How to make the organisation to adopt the changes? |
| Cloud security and privacy review  Assesses the information security practices and procedures of the cloud provider.<br>A review of security SLAs and/or an on-site vendor audit. Determines whether IT management worked to negotiate security requirements into their contract with the provider.<br>Reviews procedures for periodic security assessments of the cloud provider(s), and determine what internal security measures have been taken to protect company information and data. | Does your organisation have secure authentication protocols for users working in the cloud?<br>Have the right safeguards been contractually established with the provider? |

| | |
|---|---|
| Cloud provider service review  Assesses the ability of the cloud provider to meet or exceed the agreed-upon SLAs in the contract.<br>Areas of consideration should include technology, legal, governance, compliance, security and privacy.<br>In addition, internal audit should assess what contingency plans exist in case of failure, liability agreements, extended support, and the inclusion of other terms and conditions as part of the service contracts, as well as availability, incident, and capacity management and scalability. | What SLAs are in place for uptime, issue management and overall service?<br>Has the cloud provider been meeting or exceeding the SLAs?<br>What issues have there been?<br>Does the organisation have an inventory of uses of external cloud service providers, sponsored both within IT and directly by the business units? |

## Social Media Risk Management

| Social Media Risk Management | Key IT Internal Audit Considerations |
|---|---|
| Social media risk assessment  Collaborates with the IT organisation to assess the social media activities that would create the highest level of risk to the organisation. Evaluates the threats to the organisations information security through the use of social media. This audit may be combined with a social media governance audit to then confirm policies have been designed to address the highest risks to the organisation. | Has the organisation identited what risks exist related to social media?<br>How well are the identified risks managed or mitigated?<br>Does the organisation periodically conduct a social media audit? |
| Social media governance audit  Evaluates the design of policies and procedures in place to manage social media within the organisation. Reviews policies and procedures against leading practices.<br>Social media activities audit  Audits the social media activities of the organisation and its employees against the policies and procedures in place. Identifies new risks and assist in developing policies and controls to address the risks. | Does a governance process exist for social media within the organisation?<br>How well are policies related to social media known amongst employees?<br>Are social media activities aligned to policy?<br>What corrective actions need to be put in place given activity?<br>How does existing activity affect brand and reputation? |

## Segregation of Duties & Identity Access Management (SoD& IAM)

| SoD& IAM | Key IT Internal Audit Considerations |
|---|---|

| | |
|---|---|
| Systematic segregation of duties review audit  Evaluates the process and controls IT has in place to effectively manage segregation of duties. Performs an assessment to determine where segregation of duties conflicts exist and compare to known conflicts communicated by IT. Evaluates the controls in place to manage risk where conflicts exist | How does IT work with the business to identify cross application segregation of duties issues?<br>Are business personnel adequately informed of the ERP roles well enough to perform user access reviews?<br>While compensating controls identified for SoD conflicts may detect financial misstatement, would they truly detect fraud? |
| Role design audit  Evaluates the design of roles within ERPs and other applications to determine whether inherent SoD issues are embedded within the roles. Provides role design, role clean-up or role redesign advisory assistance and pre- and post-implementation audits to solve identified SoD issues. | Does the organisation design roles in a way that creates inherent SoD issues?<br>Do business users understand the access being assigned to roles they are assigned ownership of? |
| Segregation of duties remediation audit  Follows up on previously identified external and internal audit findings around SoD conflicts. | Does the organisation take appropriate action when SoD conflicts are identified?<br>Have we proactively addressed SoD issues to prevent year-end audit issues? |
| IAM/GRC technology assessment  Evaluates how IAM or GRC software is currently used, or could be used, to improve SoD controls and processes. | Is IAM or GRC software currently used effectively to manage SoD risk?<br>What software could be utilised to improve our level of SoD control, and what are our business requirements? |



**Data Loss Prevention (DLP) and Privacy**

| Data Loss Prevention and Privacy | Key IT Internal Audit Considerations |
|---|---|
| Data governance and classification audit  Evaluates the processes management has put in place to classify data, and develop plans to protect the data based on the classification | What sensitive data do we hold  what is our most important data?<br>Where does our sensitive data reside, both internally and with third parties?<br>Where is our data going? |
| DLP control review  Audits the controls in place to manage privacy and data in motion, in use and at rest. Considers the following scope areas: perimeter security, network monitoring,use of instant messaging, privileged user monitoring, data sanitation, data redaction, export/save control, endpointsecurity, physical media control, disposal and destruction, and mobile device protection. | What controls do we have in place to protect data?<br>How well do these controls operate?<br>Where do our vulnerabilities exist, and what must be done to manage these gaps? |

| | |
|---|---|
| Privacy regulation audit  Evaluates the privacy regulations that affect the organisation, and assess management s response to these regulations through policy development,<br>awareness and control procedures. | How well do we understand the privacy regulations that affect our global business? For example, HIPAA is potentially a risk to all organisations, not just health care providers or payers or GDPR is applicable to organizations even if they do not have operations in the EU?<br>Do we update and communicate policies in a timely manner?<br>Do users follow control procedures to address regulations? |

## Machine Learning

| Machine Learning in Internal Audit | Key IT Internal Audit Considerations |
|---|---|
| Machine learning technology helps in finding the unstructured data, which include the emails and the social media posts and review them. | What controls do we have in place to protect unstructured data e.g. emails?<br>Is there any important data leaking out through social media?<br>Where is our data going? |
| Machine learning may be applied to help with the classification of transactions. Inductive reasoning could be applied to the source data of historical transactions to help predict the classification of additional transactions as they are recorded | What is the historical transaction pattern?<br>How the transactions are been classified?<br>What are the controls to protect the historical transaction data? |
| Machine learning has the ability of the computer to recognize and apply patterns, derive its own algorithms based on those patterns, and refine those algorithms based on feedback | What is the pattern of data been processed?<br>What type of algorithms in place for analysis so it meet the requirements?<br>Does any feedback mechanism been carried? |

## Block Chain

| Block Chain in Internal Audit | Key IT Internal Audit Considerations |
|---|---|

| | |
|---|---|
| In a block chain system, the ledger is replicated in a large number of identical databases, each hosted and maintained by an interested party. When changes are entered in one copy, all the other copies are simultaneously updated. So as transactions occur, records of the value and assets exchanged are permanently entered in all ledgers. | What Existing policies and procedures will need to be updated to accommodate blockchain protocols and integrate blockchain transactions into legacy systems? |
| Blockchain technology helps to test the whole population of transactions within the period under observation. This extensive coverage will drastically improve the level of assurance gained in affected audit engagements.<br>Blockchain Uses the encryption technology which helps to secure the data. | What type of data is processed?<br>Is the data structured or unstructured?<br>What controls do we have in place to protect data?<br><br>What Credential and key management is crucial to protecting the digital assets stored on the blockchain?<br>Who will have access to the data and encryption keys? |

**Robotics Process Automation**



| | |
|---|---|
| Block Chain in Internal Audit | Key IT Internal Audit Considerations |
| RPA is configurable software, that work on the existing IT infrastructure, pulling data, performing algorithms, and creating reports. It uses business rules, can be configured to performed a variety of processes enabling multi-use robots, and variability as your business needs change. | Does the present infrastructure support RPA?<br>What are the Data Governance and Controls Standards in the context of RPA?<br>What Privacy and Data Protection the organisation follow in the context of RPA?<br>Have optimised processes before we automated? |
| RPA offers broader spectrum of internal and external application integration in risk. It help to create document repositories and connections to existing governance, risk and control (GRC) platforms that are linked to processes, risks and controls to demonstrate framework adherence and evidence traceability. | What level of control implemented to organisation on the integration of application?<br>Do business users understand the access being assigned to roles they are assigned ownership of? |

**Conclusion**

Understanding the risks in the Digital Era and mapping out a strategy to ensure that IT controls are in place is a crucial step for businesses where internal audit can play a significant role. The effectiveness of internal audit itself can be enhanced with the use of technology and tools.