Internal Audit and the Rise of Intelligent Automation

Intelligent Automation

Intelligent Automation, once an intriguing but far-fetched idea, has now become almost a given in many organisations. This technology includes robotics process automation, big data, predictive analysis and machine learning, to automate knowledge work. Different organisations across all sectors are now investing widely in intelligent automation.

The transformation process of Intelligent Automation creates many competitive advantages for an organisation. For example, chatbots and robo-advisors in a customer service operation enables timely engagement of customers; automatic claim processing in an insurance business increases workforce capacity; automated billing in the utilities sector lowers labour costs; and patient scheduling systems in healthcare improve efficiency.

Highly adaptable and customisable for businesses, the spectrum of Intelligent Automation spans from basic process automation to enhanced automation and comprehensive cognitive automation.

RULES

Basic process automation

- *Extraction of information at the screen and document level*
- *Workflow automation*
- *Self-executing processes*

LEARN

Enhanced automation

- *Learning capabilities*
- *Ability to work with unstructured data and read source data manuals*
- *Natural language recognition and processing*

REASON

Cognitive automation

- *Artificial intelligence*
- *Self-optimising*
- *Predictive analytics / hypothesis generation*
- *Supervised learning*

The use of Intelligent Automation is happening and is accelerating quickly. The question is – what is internal audit's role in this transformation?

Internal Audit's Role in Assessing Intelligent Automation

Intelligent Automation can significantly transform how business is done. However, without proper design, operating guidelines and monitoring, Intelligent Automation may fail to achieve its design goals or cause unintended destruction to the business, such as data leakage. To avoid this, the internal audit function plays a critical role by providing assurance over this transformation.

It is vital for internal auditors to be able to identify the relevant risks that may disrupt the success of Intelligent Automation. In order to do so, internal auditors must first establish a solid understanding of the end-to-end Intelligent Automation Development Lifecycle to ensure that they have the capabilities to profile the relevant risks.

This Lifecycle can be illustrated via an iterative process of plan, build, test and operate.

The Intelligent Automation Development Lifecycle

The Lifecycle – of plan, build, test and operate – is a process that relies on on-going data feeds and confirmative programming to ensure the technology continues to produce the desired decisions and outcomes.

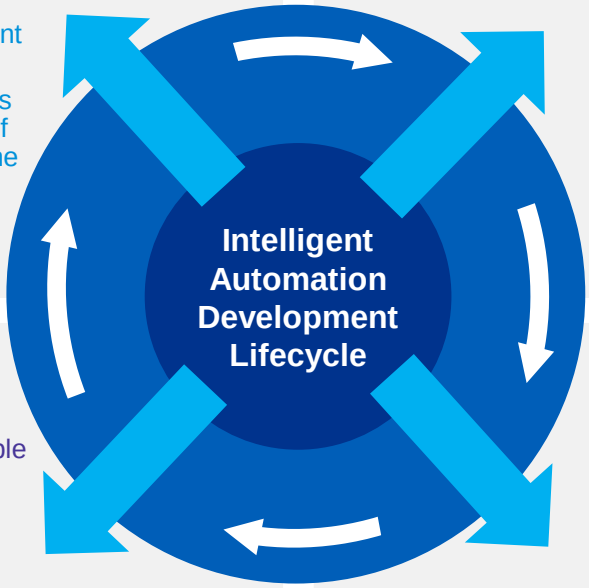
Based on the Lifecycle, the following are common risks that we have noted:

Plan

- Misalignment of Intelligent Automation initiative with strategic objectives
- Gap between problems and resolution capabilities
- Inaccurate vendor assessment and incongruent vendor selection
- Improper budgeting process and inaccurate projection of return on investments on the Intelligent Automation programme

Build

- Regulatory non-compliance (e.g. data protection / privacy)
- Misunderstanding of user requirements and objectives
- Limited understanding of model function and training to explain the application's decision logic
- Lack of clarity on roles and responsibilities, including bot and data ownership



Operate

- Inadequate monitoring of Intelligent Automation bias for departures from the intended output or acceptable conduct
- Inappropriate interpretation of data and erroneous application of evidence and probability algorithms
- Improper data governance framework resulting in corruption / contamination of the Intelligent Automation solution
- Unauthorised system manipulation / data access, and lack of appropriate exception reporting and communication

Test

- Lack of segregation of duties between design and testing to prevent undetected user bias
- Insufficient intelligent automation training during User Acceptance Testing to fully understand risks and implications
- Inability to forecast machine learning or understand and explain the application's learning methodology
- Requirement for continuous testing and monitoring as Intelligent Automation inherently adapts results based on new data provided due to machine learning capabilities

Bearing in mind the common risks noted above, obtaining assurance over Intelligent Automation outputs in the Intelligent Automation Development Lifecycle requires three key actions by the internal auditors: verification, validation and control.

1 Verification

Is the application executing only the prescribed specifications?

2 Validation

Were correct and appropriate specifications chosen for the model?

3 Control

Can the human operator effectively monitor and correct the system as needed?

KPMG's Intelligent Automation Audit Framework

In recognition of the new risks introduced by Intelligent Automation and the aforementioned actions that should be taken by internal auditors, KPMG has established an Intelligent Automation Audit Framework to assist enterprises in defining and managing these risks.

Key Considerations within the Framework

Model Management

- Is complete, representative and high quality data being fed to the model to form the basis of the model decisions?
- Who in your organisation fully understands the logic within the model?
- Is there a rollback functionality to manually reverse or amend the outcome if necessary?
- Is there adequate testing / validation of models?

Strategy and Governance

- Are Intelligent Automation investments and outcomes aligned with the business objectives and strategies?
- How are new risks of Intelligent Automation addressed in the design and compliance with relevant regulations, policies and procedures?
- Is there an appropriate owner identified to be accountable for the programme?

People and Talent Management

- How will you recruit, develop and retain the human resources required for an effective Intelligent Automation enabled environment (e.g. data scientists and software developers for deep learning and coding)?
- Is a change management process in place to help employees to understand, commit to, and embrace Intelligent Automation?

Supplier and Third Party Management

- Do you have a high reliance on specific vendors that can result in single dependency and concentration risk?
- Is there full on-going visibility of all parties involved in providing the overall Intelligent Automation solution?
- Is there clear documentation on ownership of intellectual property, i.e. data, models, bots?

Business Operations

- How suitable is the process for Intelligent Automation implementation and what error handling and resolution plans exist when needed?
- Are there any Intelligent Automation-specific performance indicators to record and monitor system performance?
- Does the organisation have a tried and tested response plan to restore business-critical processes and functions that rely on Intelligent Automation to avoid or minimise the impact on business operations and financial loss?

KPMG's Intelligent Automation Audit Framework (continued)

Security and Data Management

- Are there appropriate access controls, especially for third parties to prevent data leakage risk in a shared infrastructure?
- Is it possible for the Intelligent Automation solution to become corrupt based on the data it receives?

Information Technology Operations

- Does your IT function maintain a complete and accurate inventory of all Intelligent Automation assets in order to manage its risks and to ensure resilience of your Intelligent Automation solutions?
- Do you have any resources and expertise to manage system outages, non-availability of data, or IT security breaches?

Key Takeaways

- Intelligent Automation is bringing sweeping changes to business operations. Hence, internal audit functions must develop strong capability in continuous monitoring to identify such initiatives that are occurring within the business in a timely manner.
- Internal audit functions need to acquire the skills to provide assurance. It must have sufficient knowledgeable and skilled internal audit professionals to prepare, oversee and reduce critical risks arising from the implementation of Intelligent Automation in the business.
- Internal audit functions must be able to establish a holistic view of risks across the Intelligent Automation Development Lifecycle by ensuring strong process walkthroughs are conducted, in order for auditors to understand whether the right controls have been designed and operating effectively.

How does KPMG Help?

FRAMEWORK

Assist internal audit functions to develop a Risk & Control Matrix and an approach to provide assurance

Provide quality assurance review over coverage of Intelligent Automation planning, execution and audit activities

REVIEW

TRAINING

Deliver training to the business, operations and control teams to successfully execute and oversee Intelligent Automation strategies

Deliver end-to-end Intelligent Automation audits as an outsourced or co-sourced partner

AUDIT

Contact Us

Alva Lee
Partner
Risk Consulting
KPMG China
T: +852 2143 8764
E: alva.lee@kpmg.com

Jia Ning Song
Partner
Risk Consulting
KPMG China
T: +852 2978 8101
E: jianing.n.song@kpmg.com

Henry Shek
Partner
IT Advisory
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Karan Kumar
Director
Risk Consulting
KPMG China
T: +852 2847 5166
E: karan.kumar@kpmg.com

Bhagya Perera
Director
IT Advisory
KPMG China
T: +852 2140 2825
E: bhagya.perera@kpmg.com

Jee Eu Tan
Associate Director
Risk Consulting
KPMG China
T: +852 2847 5182
E: jeeeu.tan@kpmg.com

kpmg.com/cn