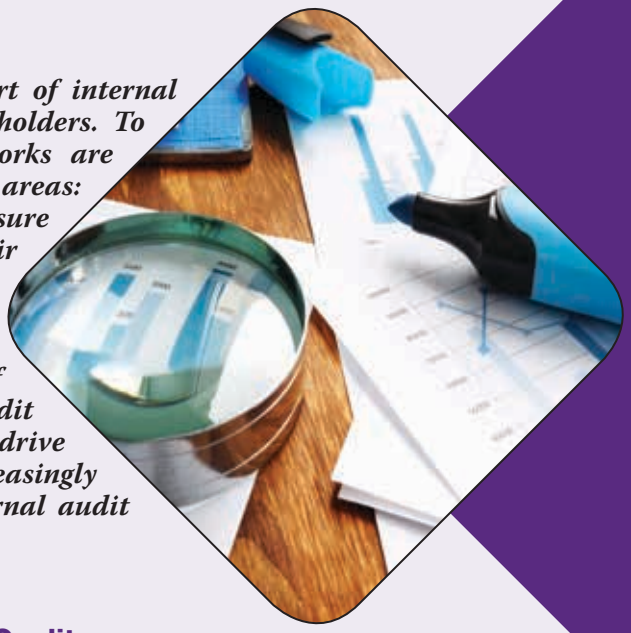
Internal Audit in the Age of Data Analytics



Effective analysis of data must lie at the heart of internal audits if they are to remain relevant to stakeholders. To make this happen strong governance frameworks are needed on data analytics, covering four key areas: quality, talent, independence and security. To ensure that organisations are getting the most from their investment in analytics, they must review their governance frameworks with a view to adopting a more transformative approach. Fast-evolving technologies that generate increasing amounts of data have created an opportunity for internal audit departments to leverage data to evaluate risk and drive audit insight. As a result, data analytics is increasingly becoming an indispensable element of the internal audit toolset.

The Need for Data Analytics

Analytics breaks down vast volumes of data and then rebuilds it to form information clusters that the auditor can use to analyse the risk landscape.

Effective data analytics elevates performance, provides greater value to the organisation, and increases the credibility of an internal audit with its stakeholders. It is also helping to transform internal audits by significantly automating processes, supporting compliance within existing organisational policies, and providing management with a higher level of operational assurance.

However, such opportunities are often coupled with risks, and this area is no exception. In making the most of data analytics, internal audit departments face issues, including: inaccurate or misleading results; misuse or misinterpretation of data; conflicts in independence; development of talent; and challenges around data privacy and security.

To address the above, internal auditors should focus on effective analysis of better data and strengthen their internal audit governance framework to cover emerging data-analytics-related risks surrounding quality, talent, independence and security.

Courtesy ICAEW Online Assurance Resource. Comments can be sent to eboard@icai.in

Quality

High quality, impactful analytics are an asset to the business and a boon to the credibility of internal audits. Unfortunately, trust can be rapidly lost due to inaccurate or unreliable results, which can be caused by poor quality data; incorrect coding; poor or misleading presentation; and failing to answer the question. It is, therefore, imperative that testing and quality assurance (QA) procedures are put in place that take into account the 'quality' risks attributed with developing an analytics solution.

A strong test and QA framework should incorporate principles from the IT development cycle, including:

- Data quality standards and assessments. For example: Service Level Agreements (SLAs) for regular data deliveries; direct access to validated data sources (data warehouse or Enterprise Resource (ERP) applications); header row counts; and data-quality profiling for key attributes.
- Code verification. For example: logical accuracy and correctness, and formats.
- Output validation. For example: checks that the output answers the business problem; output readability; and consistency.

Some organisations that are more advanced with their use of data analytics are starting to develop data-quality assessments and standards at macro (general content) and micro (specific fields or values) levels. The purpose of these assessments is to identify erroneous data and to measure the impact on analytics-driven processes. It is critical to identify data errors and to understand their implications.

The quality assurance scope should include the tools (and algorithms) used for performing the analysis of data. The objective is to get assurance that these tools operate as intended.

Talent - Roles and Responsibilities

Analytics is most effective when there is close engagement between internal auditors and data analysts. Whenever the roles and responsibilities between analytics specialists and auditors are not well defined, there is a risk that the relationship becomes unbalanced and ineffective. For example, too little involvement from analytics in defining the audit scope can result in inappropriate insights being produced, whereas an over-reliance on analytics to define the testing can lead to the wrong questions being asked or risks being investigated.

Analytics is most effective when there is close engagement between internal auditors and data analysts. Whenever the roles and responsibilities between analytics specialists and auditors are not well defined, there is a risk that the relationship becomes unbalanced and ineffective.

To achieve the right balance of responsibility and collaboration between data analysts and auditors, there should be clarity in terms of the roles that they each perform. In addition, organisations should align performance goals with the broader goals of the data analytics initiative.

Through training and skills development, the capabilities across internal audit team members should converge to share a common understanding of tasks and behaviour. For example, traditional auditors should be in a position to not only handle appropriately sensitive data provided by data analysts, but also interpret and communicate to the business results produced by data analyst. Similarly, data analysts should collaborate with auditors to enhance their understanding of data sensitivity and produce more effective analytics.

Independence

It is imperative that use of data analytics must preserve the internal auditor's independence and objectivity. The nature of the outputs delivered by the analytics cycle can give rise to specific complications when it comes to meeting these principles. Careful consideration must be taken to address a number of issues that can affect the independence of the audit work.

It is imperative that use of data analytics must preserve the internal auditor's independence and objectivity. The nature of the outputs delivered by the analytics cycle can give rise to specific complications when it comes to meeting these principles. Careful consideration must be taken to address a number of issues that can affect the independence of the audit work.

For example, an analysis that identifies specific instances of control failures could arguably be interpreted by the business as part of a detective control. In fact, often it is the business that first approaches the internal audit function to learn how analytics can be transferred down the lines of defence.

Although internal audit does not own any data sourced to produce the analyses, it does own the outputs and the respective logic used. If the logic is transferred in full, directly to the business, how does that impact the internal audit function's independence and objectivity when reviewing the same area later down the line? How does the business and its internal audit function share common data platforms, repositories and tools?

It does not make economic sense for internal audit functions to build their own infrastructure, the build and maintenance costs are excessively prohibitive. Multitenancy approaches that allow a single data platform (such as a data lake) to serve multiple tenants or departments are being explored by an increasing number of organisations. The tenants do not share or see each other's data.

An organisation's data analytics governance framework should consider the disruptive influence of analytics on the relationship between audit and business. A collaborative approach should be considered, but with clear roles and responsibilities for data sourcing and access, data knowledge, and data quality.

Data Security and Processing of Sensitive Data

As large data consumers, the internal audit team is exposed to the same risks around data security and privacy that it examines for its stakeholders. Managing these risks becomes doubly important when dealing with the additional complications arising from jurisdiction-specific regulation and cross-border issues.

As large data consumers, the internal audit team is exposed to the same risks around data security and privacy that it examines for its stakeholders. Managing these risks becomes doubly important when dealing with the additional complications arising from jurisdiction-specific regulation and cross-border issues.

Although the department will already have policies surrounding collection, storage and disposal of audit working papers, internal auditors should consider these policies with respect to the end-to-end data analytics lifecycle and for each data class define:

- what data can be requested/stored;
- how data is accessed;
- who can access the data on the storage platform(s);
- where the data can be stored;
- what data can be distributed or transferred and to whom; and
- the data retention period.

Particular attention should be given to how personally sensitive data is processed and stored, such as client identifying data, taking in account jurisdictional regulations or cross border restrictions. This is especially relevant to organisations whose analytics organisational model includes offshore centres of excellence.

In addition, the data analytics governance framework should encapsulate the preservation of the three major concepts in information security: confidentiality of data stored, processed and reported; data integrity; and data availability. In the case of any breach, the organisation should be in a position to take corrective actions as soon as possible.

It is also worth noting that sourcing and collating data for the purpose of analytics could result in increased cyber security risk. Besides insider threat, privileged users (including data analysts) who have access to an organisation's crown jewels (such as customer sensitive data) can be targeted by cyber criminals. To mitigate this risk, organisational policies, such as encryption of sensitive data, should be complied with by all privileged users including internal auditors and data analysts.

Conclusion

Data analytics is transforming audit by providing data-enabled insight coupled with automatic identification of high-risk items, allowing auditors license to prioritise and investigate high-value areas.

Data analytics is transforming audit by providing data-enabled insight coupled with automatic identification of high-risk items, allowing auditors license to prioritise and investigate high-value areas.

More importantly, a higher and unprecedented level of efficiency is achieved by letting analytics focus on transactional and low-value activities, with auditors focusing on high-risk items that require critical human observation and examination.

As well as the benefits in disrupting traditional audit processes, analytics also brings with it a number of inherent risks that can limit effectiveness or expose the department to reputational damage.

The starting point for managing these risks should be the careful review and development of a governance framework that helps align use of analytics to audit strategy and risk appetite.

The governance framework should articulate:

- clear roles and responsibilities in relation to the resources involved in the entire analytics process;
- address conflicts of interest issues that could potentially arise; and
- describe how issues will be resolved.

As data and analytics are key components in the evolution of internal auditing, the governance framework must then be incorporated in the organisation's internal audit methodology. ■

I know God won't give me anything I can't handle. I just wish he didn't trust me so much. - *Mother Teresa*