GLOBAL KNOWLEDGE BRIEF

INTEGRATING A DATA-DRIVEN APPROACH: LEARNING THE BASICS

Fundamentals of building data analytics into the internal audit methodology

The Institute of Internal Auditors | Global

Table of Contents

INTEGRATING A DATA-DRIVEN APPROACH: LEARNING THE BASICS

Fundamentals of building data analytics into the internal audit methodology

Introduction

The amount of data that organisations produce and accumulate grows larger every year, and the tools and technologies to turn that data into useful information continue to advance. Successful internal audit departments must be able to grow their capabilities to harness those tools and technologies and use the vast amount of data in their organisations to provide greater levels of assurance and value-added services, all the while improving the efficiency with which they do so.

IIA Standards Glossary

Data Analytics

A process of inspecting, cleaning, transforming, and modeling data with the goal of highlighting useful information, suggesting conclusions, and supporting decision-making.

The best way to implement a data analytics methodology is to manage it like a project championed by the chief audit executive (CAE). By involving the organisation's IT department, data management staff, project managers, and business owners, internal audit can build the constituency needed to be successful.

CAEs must realistically map the project to acquire the information needed, and get the permission of the business owners to access the data. CAEs must gain the support of IT, and define the skills required on the internal audit team to be data analysts. Beginning analysts might rely on spreadsheets, then advance to using tools designed for data analytics, and ultimately fluently use databases and write ad hoc scripts. CAEs must recognise opportunities exist for ambitious, technologically inclined professionals.

Internal audit functions that challenge themselves to be leaders in the field of data analytics will enjoy the fruits of being leaders in their organisations and in the profession of internal auditing.

THE BASICS

Data analytics improve the efficiency and effectiveness of the audit program

Making the business case for analytics

Undertaking the effort to transform an internal audit department to one with a data-driven methodology is absolutely an investment. Chief audit executives (CAEs) who pledge to improve their department's capabilities through data analytics must commit to:

- Set aside time to understand the organisation's data architecture and infrastructure.
- Continuously stay on top of changes to the data that the organisation maintains.
- Provide training to new and existing staff.
- Hire professionals comfortable with a data-driven methodology.
- Acquire data tools and technologies capable of performing analytics.
- Provide continuing professional education to team members to stay abreast of advancements in tools and techniques.

While the commitment to mature to a data-driven methodology is significant, the opportunities for the internal audit function are equally significant. Internal auditors who include data analytics and transform their audit methodology to be data-driven are better positioned to:

- Improve the quality of their risk assessments.
- Provide greater levels of assurance to their management, board of directors, and other stakeholders.
- Identify significant, but infrequently occurring, issues in business processes.
- Enhance the quality of recommendations.
- Be more efficient in executing their audit plan.

CAE role

The CAE is responsible for developing a comprehensive vision for the internal audit department, including its commitment to having a data-driven methodology. That vision should be developed with consideration of the needs of key stakeholders, including the audit committee, senior management, and regulators, if applicable. It cannot be accomplished without the buy in of the organisation, the necessary support from IT, and permission from the data owners to access the data. Once developed, the CAE is responsible for ensuring that the vision is effectively communicated across the department and within the organisation.

The level of commitment to a data-driven methodology includes determining the level of investment in data analytics that is appropriate for the organisation's internal audit function. However, it is not enough to establish, communicate, and provide resources to support the vision of having a data-driven methodology. The CAE must also continually monitor the performance of the department against the established vision.

By setting the expectation that audit conclusions and recommendations be supported by applicable data, the CAE is able to promote a culture where data is the basis for decision-making. While it is not always necessary for the CAE to have the knowledge to use the specific tools to execute data analytics, the CAE should have the capacity to provide guidance on the types of queries and analytics that will adequately support internal audit communications. Further, the CAE should ensure that job descriptions and hiring decisions support the hiring of professionals who can elevate the department's data analytics capabilities.

TYPES OF ANALYTICS

Opportunities to integrate

Start with commitment

Once an internal audit department has committed to, and prepared itself for, being data-driven in its methodology, there are opportunities in the development of the audit plan and nearly every type of engagement in the audit plan to improve the quality and efficiency of its engagements. Data analytics can particularly facilitate tasks such as fraud detection and investigation, operational performance, compliance, and internal controls. Internal auditors, under the leadership of their CAE, should continuously seek ways to turn the organisation's data into usable audit information.

IIA Standards Glossary

Risk Assessment

The identification and analysis (typically in terms of impact and likelihood) of relevant risks to the achievement of an organisation's objectives, forming a basis for determining how the risks should be managed.

Improved risk assessments

Risk assessment is fundamental to the work of internal audit. Periodic, or continual, enterprisewide risk assessments form the basis for the audit plan. Engagement level risk assessments help define the engagement work program. Each of these types of risk assessments can become more effective and efficient with the use of data analytics.

Determining the audits that should be included in the audit plan based on the entire audit universe is one of the most critical decisions a CAE must routinely make. Using data available within the organisation, the CAE can validate, or disprove, qualitative assessments of risk gathered through interviews and discussions. Further, analyses of trends can identify emerging risks that have not yet manifested themselves, allowing the internal auditor to perform engagements and make recommendations to improve increasingly important processes to help their organisations achieve stated objectives.

During the planning phase of an engagement, internal auditors develop a work program. The work program defines the procedures to be performed, procedures that may include data analytics. However, data analytics also can be used effectively to develop the work program during planning. Analyzing data regarding the business unit or process to be audited allows the auditor to develop a work program that is focused on the highest risks.

For example, if an internal audit department is planning an engagement of its accounts payable processes, it may start by analyzing payment trends, looking at number of vendors, speed of payment, late charges

incurred, discounts missed, etc. By performing these analyses during planning the auditor can focus the procedures in the work program on the highest risk areas, and become more efficient by reducing scope on less risky areas.

Fraud considerations

The IIA's *International Standards for the Professional Practice of Internal Auditing* require internal auditors, during engagement planning, to consider a number of exposures, including the probability of fraud, when determining the engagement objectives. When auditors determine the probability of fraud to be worthy of inclusion in the audit work program, the use of data analytics should be considered.

Data analytics provides the ability to test entire populations as close to real time as possible. Data-mature internal audit departments continuously identify sources of data and determine how to analyze that data. The ability to evaluate full populations of transactions makes data analytics a key tool for internal auditors to utilize to potentially detect fraud.

Data analytics designed to detect fraud need not always be completely distinct from procedures designed to evaluate others determined in the engagement planning. For example, in a procure-to-pay audit, the auditor may use data to determine compliance with adherence to transactional approvals. That same data set may be utilized to compare vendor addresses to employee addresses to identify potential fraudulent payments to fake vendors.

Audit Focus

IIA Standard 2210: Engagement Objectives

Objectives must be established for each engagement.

2210.A1: Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

2210.A2: Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

In addition to engagements included in the internal audit plan, auditors may be called upon to perform investigations where fraud is alleged or suspected. In these cases, the internal auditor should give strong consideration to using data analytics tools to prove or disprove an allegation of fraud.

Enhanced operational process auditing

Data analytics can be particularly useful in expanding the capacity of an internal audit function to perform process assurance engagements. Whereas traditional sampling techniques force the auditor to sample from potentially very large populations and draw conclusions based on the samples, data analytics allow the auditor to perform tests on entire populations. Additionally, the auditor can use pre-determined criteria to identify transactions that are higher risk and to which additional audit procedures may be necessary.

Data analytics are of particular value in instances where significant risk may occur in low frequencies. The auditor can use analytics tools to identify those small number of high-risk transactions and properly allocate audit resources to evaluating those transactions.

Further, internal auditors have the ability to use data analytics to provide greater insight into the operational performance of processes under review. While process owners may track a limited number of key performance indicators, internal auditors may have the ability to dive even deeper into the relevant data to provide

management with greater insight into its performance. For example, in a procure-to-pay audit, the auditor may use data to determine the extent to which available early pay discounts were utilized.

Taking financial auditing to the next level

Internal auditors involved in performing traditional financial auditing — whether it be in support of specific compliance requirements, assisting external auditors, or providing assurance to its management and audit committee — can enhance their efficiency and effectiveness using data analytics. Data analytics can be used in financial audits in various manners.

Traditionally, auditors used various techniques to develop a sample of transactions or balances intended to be representative of the population or to gain adequate coverage for materiality. Testing exceptions were used to identify potential deficiencies. In the rare cases that statistical sampling was used, the exceptions rates could be extrapolated across the population. While statistically valid to extrapolate results of a statistical sample to a population, stakeholders are often less confident about relying on extrapolated results.

Internal auditors can use data analytics to improve sampling techniques, by analyzing entire populations of transactions and selecting only those items that meet pre-determined, risk-based criteria for testing.

When data analytics are used, opportunities exist to evaluate whole populations of transactions and balances. Because the entire population of data is evaluated, the size and scale of deficiencies, if identified, can be communicated without the need for extrapolation.

Areas where data analytics can be used to enhance financial audits include:

- Sampling journal entries that meet certain risk factors, including size, timing, key accounts, etc.
- Selecting transactions near cut-off periods.
- Identifying transactions that do not meet the organisation’s approval requirements.
- Analyzing the aging of transactions such as accounts receivable, accounts payable, construction in process, and notes receivable.
- Testing calculations of depreciation, amortizations, subscription-type revenue recognition, and interest accruals.

Consulting and advisory engagements

In addition to process assurance and financial auditing engagements, audit departments often provide consulting and advisory engagements. It is in these types of engagements where internal auditors can become most creative in their use of data analytics. Auditors can use their knowledge of business processes and the underlying data available to design analytics that support value-added recommendations.

The nature and scope of data analytics are only as limited as the imagination of the auditor. CAEs should foster a culture where auditors are challenged to ask questions and then use the data available to them to seek answers.

Continuous auditing

Internal audit functions whose capabilities in the use of data analytics have matured, may elect to employ continuous auditing techniques. Continuous auditing involves establishing scripts that run perpetually. They are typically designed to identify transactions that meet certain criteria that have been determined to be worthy of further investigation by an auditor. The established criteria may indicate non-compliance with a policy or may be indicative of a potential improper transaction. While, the nature of continuous auditing scripts will vary based on the nature of the organisation and its specific risks, examples include scripts to identify:

> **IIA Standards Glossary**
>
> **Continuous Auditing**
>
> **Using computerized techniques to perpetually audit the processing of business transactions**

- Journal entries that occur late or at unusual times.
- Transactions without necessary approvals.
- Transactions very near approval limits, including potential split transactions.
- Inappropriate vendors.
- Failure to adhere to payment terms and/or missed discounts.

Management assistance

As internal audit departments develop a reputation for being data-driven trusted advisors, they may get requests from management to analyze data in support of projects or key initiatives. It is the responsibility of the CAE to ensure that the internal audit function maintains its independence and objectivity. In the analysis of data, internal auditors may be able to add significant value. They can aid with regard to executing data analysis at the request of management and can make recommendations for process improvements. However, they should never be in a position where they are designing or implementing controls.

> **IIA Standards Glossary**
>
> **Continuous Monitoring**
>
> **The automated review of business processes and controls by associates in the business unit. It helps an organisation detect errors, fraud, abuse, and system inefficiencies.**

In addition, process owners may elect to employ continuous monitoring techniques, which are similar to continuous auditing techniques, but are performed by and are the responsibility of management, and its staff. Generally, the implementation of continuous monitoring is indicative of strong management monitoring of internal controls. Internal auditors may be interested in promoting strong monitoring activities and can provide consulting in the design of continuous monitoring. However, the ultimate responsibility for the design and operational execution of monitoring activities must continue to rest with management. Further, internal auditors may be called upon to perform engagements that include evaluations of the adequacy of management monitoring activities to reduce risk to the organisation.

PERFORMING ANALYTICS

Data identification and preparation

Building a plan

Once an internal audit department commits to a data-driven methodology, adopting a data-driven approach should be managed like any other investment or implementation. There must be a project plan to lead the effort, from planning, designing, and implementing all the necessary elements: technology, training, resources, security, etc.

As internal audit develops the "how" aspects of executing efficiently and effectively, several aspects should be considered. Because the nature of each organisational culture, objectives, industry, regulatory environment, and internal audit activity varies so greatly, it is important for each department to build its own unique game plan. However, CAEs should leverage what has been learned by peers. The greatest learnings from prior experiences can be gained from networking, particularly with industry peers. While the details of data are proprietary, internal auditors within an industry group should be open to sharing data analytics approaches and lessons learned.

Understanding the data

A common mistake for internal audit departments diving into data analytics for the first time is not budgeting adequate planning time to gain a full understanding of the data that is available and not partnering with IT. Most internal auditors are able to gain an understanding of how transactions in their organisations generally flow between systems. However, they rarely get in the fine detail of the format and location of where data is stored in databases. Many organisations store their data in relational databases that require users of that data to understand how the data is mapped.

Much of the transactional data that auditors utilize in their analytics, including that which comes from relational databases, or even spreadsheets, is available in a highly organised manner. This type of data is generally referred to as structured data. Structured data is that which is accumulated and stored in an organised, and often readily searchable, methodology. With structured data, fields store length-delineated data such as account names, transaction amounts, employee ID numbers, etc. Structured data usually also contains text fields of variable length like addresses that are contained in records. While work may need to be done by auditors to bring structured data into formats usable by the auditors' preferred tools, structured data is generally much easier to use than unstructured data.

Unstructured data is essentially all other types of data. This can include data that is accumulated in emails, contracts, social media posts or any other types of free form data. The challenge for auditors is determining how to convert unstructured data into a structure that facilitates using data analysis tools. The types of

unstructured data that may be useful to an auditor is infinite. The manner in which auditors convert unstructured data to a useful structure varies by the nature of the data, but may include specialized search tools. However, in some cases, auditors may need to employ time-consuming manual processes. For example, auditors may need to review contracts and extract key components and populate simple databases with key terms or other components of the contract.

Another challenge that internal auditors frequently face is the sheer size of data available to them. The term data lake was created by James Dixon, the founder and CTO of Pentaho, to describe a data storage repository that holds a vast amount of raw data in its native format: "If you think of a datamart as a store of bottled water – cleansed and packaged and structured for easy consumption – the data lake is a large body of water in a more natural state. The contents of the data lake stream in from a source to fill the lake, and various users of the lake can come to examine, dive in, or take samples."

The beauty of executing a data-driven approach is the ability to perform tests on the full population of data or a very large subset of it. Yet, organisations with tetrabites of data are particularly challenging for internal audit, when it comes to the notion of collecting data, and the sheer size of data available to an internal auditor can be overwhelming. If not paired down to what is truly needed, the data may test the computing power of equipment available to the auditors or make the analytic intended impossible to perform.

When selecting data to perform analytics, auditors should be careful to pull in all fields necessary to execute the test, but minimize the number of unnecessary fields. Further, proper selection of records to use in the analytic can make the size of the data set usable. It is often advisable to test the analytic on a relatively small data set. For example, if the auditor is seeking to test a year's worth of transactions, they might want to start with a week or a month to ensure that the analytic works as intended. Further, eliminating records from the analytic that do not contribute to the analysis can reduce the computing capability needed. An auditor may consider, for example, reducing immaterial small value transactions to ensure it is possible to analyze larger and more significant transactions.

Data preparation

Formatting

Auditors should be familiar with the data format needed to perform analytics in the tool that they have selected to use, recognising that this may not be the native format in which the data is collected and stored in the organisations' systems. Where this is the case, auditors must budget time to prepare the data for usage and be familiar with tools to accomplish this.

Frequently, specific analytical procedures using data require the user to leverage data from separate sources. A failure to understand how those pieces of data can be compared can cause significant delays and inaccurate results. Further, the internal auditor must gain an understanding of what data is available, over what time period it is available, which systems it was generated from, and in what databases it resides.

For example, if the auditor wants to perform a fairly simplistic test, they might want to compare addresses in the organisation's vendor master file to payroll records to see if there are any employees who have set up dummy vendors to create fraudulent charges. On its face, this should be a fairly simple exercise of merging records from payroll systems to records in the vendor master file. However, if the two different systems format addresses in a different manner, it can cause significant confusion. One system may put different components of the same address in different fields, such as city and zip code, whereas the other system stores the entire address in the same field. In this case, the auditor would need to understand that difference and take the time to format the data so it is comparable.

Validating

Once an auditor believes that they have accessed and prepared the data and are ready to perform analytics, it is imperative that they validate the completeness and accuracy of the data that they have prepared. There are a number of ways to accomplish this and the specific steps will be unique to each data set. Common checks include:

- Validate that the number of records is consistent with the data source.
- Perform hash totals for numeric fields to be utilized and compare to source data.
- Check for blank fields or appropriate data type (numeric or text fields where appropriate).
- Compare arithmetic means or medians for key numeric fields to ensure that they are within the range of expectation, based on knowledge of the business.

Independent collection of data

To the maximum extent possible, internal audit departments should acquire the access and develop the knowledge and skills to acquire data from organisational systems directly. However, this is not as easy as it sounds. To achieve this ideal situation, auditors must understand not only where data is, but how to harvest the data within the organisation's systems and using the department's tools.

Appropriate access should be granted to allow the auditor to access all data, but ideally restrict the ability to initiate transactions or modify data in systems. In many organisations, internal audit management works with information systems personnel to design access profiles suited to internal audit team members.

Evidence gathered directly by an auditor is generally stronger than evidence gathered and shared under the direction of members of management. This is certainly true with regard to data requests. Hence, while it may be more time consuming, especially at first, for internal auditors to source their own data from organisational systems, it is preferred from a quality of evidence perspective.

Further, data analytics is often an iterative process, with trial and error being a common approach to designing analytics. When auditors have the ability to source their own data, they are not dependent on the schedules and availability of management resources to fulfill ongoing requests for data. In addition, to the extent that the nature and timing of audit procedures are not ideally communicated to management, this sourcing of data can be performed without other communications.

Collaborating to collect data

While the independent sourcing of data for use in analytics is certainly ideal, it is not always possible. This is particularly true in departments that have not reached a high level of maturity with regard to their data analytics program. This may also be true in relatively small departments, where there are not auditors knowledgeable about how to access the data, or where an investment in data specialists is limited.

A collaborative approach is best in cases where internal auditors are dependent on information technology and/or management personnel to source data. Recognise that in most situations, personnel being asked to source data for auditors are performing work above and beyond their normal responsibilities. It is most efficient for the organisation to be clear on the requests being made and the deadlines for requests to be met. Be thoughtful of setting deadlines that are truly necessary.

Good practice is to not only make specific requests, but also work with data owners to communicate the intention of what the auditor is looking to accomplish. Data owners, who are more familiar with the data, may be able to identify specific fields that are necessary. Similar to performing certain analytics for the first time, it is advisable to have a sample of the population extracted so that the auditor can evaluate if it will fulfill the objective of the analytic.

Whether collecting data independently or working with other organisational personnel, it should be the auditor's objective to acquire all data necessary to perform their work in the most efficient manner possible. The single largest challenge to efficient data collection is not understanding what is necessary and having to repeatedly perform extraction exercises.

Data security and privacy

As in all work, when collecting data, internal auditors must be cognizant of their collecting and handling of sensitive data.

Certain analytics may require the use of personally identifiable information (PII). This commonly used term in North America refers to a somewhat narrow range of data such as name, address, birthdate, telephone number, email address, and financial information, such as bank account and credit card numbers. Yet, it's a different situation in the European Union. The EU General Data Protection Regulation (GDPR) defines "personal data" more broadly, and can include social media posts, photographs, and lifestyle information. The GDPR defines personal data as:

> Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.

To the extent that an auditor must use PII to perform analytics, special precautions should be made with regard to the handling and access to such information. When PII is available in a data source that is being used but is not required to complete the audit step, auditors should consider excluding those fields from the data set used to perform the analytic.

Most organisations utilize employee numbers which are unique to an employee. When this is the case, use that number as the unique identifier for an employee record. If it is later necessary to identify additional PII about a specific employee, auditors can tie the employee number back to a specific individual for further work. This may require the assistance of human resources personnel.

In addition to PII, there are various other forms of sensitive information that may be available to auditors and require particular attention, such as compensation or employee evaluations. Further, auditors may have access to competitively sensitive data and material non-public information, such as sales and cost figures. Auditors should be cognizant that these types of data need to be handled with particular care, even within the department.

Internal auditors must understand organisational policies and procedures with regard to sensitive information and records retention. CAEs should also consider establishing departmental policies and procedures on how to gather, utilize, and store sensitive information, specific to the manners in which internal audit works. Internal audit policies should not be in conflict with organisational policies, but instead should be complementary.

DATA ANALYSIS RESOURCES AND TOOLS

Finding the right resources

What does your team need?

The investment in tools and technologies required to meet internal audit's objectives and the staffing needed to perform data analytics are key decisions to be made by the CAE, decisions that are unique to each internal audit department.

Some departments utilize dedicated staff or even a team of staff members to perform data analytics. Other departments cross-train some or all staff members, to execute data analytics. The decision as to whether to have dedicated data analytics team members, or even a team of data analysts, is typically driven by budgetary constraints. Larger, more mature internal audit functions working in large, highly regulated environments are more likely to have the resources to dedicate to data analytics. CAEs of smaller internal audit departments, working in less complex or less regulated environments, may not have the resources at their disposal to fully dedicate team headcount to data analytics.

For data analytics, a wide variety of tools are available. Some are common tools, such as spreadsheet programs that are readily available. In addition, many specialized tools exist, particularly catering to internal auditors and data analytics professionals. Which tools are appropriate for a particular internal audit department or internal auditor is a decision that must be made by the CAE, recognising needs and budgetary constraints.

And CAEs cannot forget to recognise the need for the internal audit department to ramp up its own data storage systems to securely store and analyze the large amounts of data it is collecting.

Using spreadsheets

Spreadsheet applications, standard tools provided to all auditors and professionals in work computers, are excellent programs to perform basic data analytics. While some functionality of spreadsheet programs may require auditors to invest some time in researching or getting specialized training, most auditors have a basic knowledge of using spreadsheets and can perform analytics with little or no training.

Modern spreadsheet applications have user-friendly functionality to do basic tasks. Internal auditors can import data easily into spreadsheets, and merge and split data fields, commonly referred to as columns. Further, basic functionality is available for sorting, querying, and calculations.

The limitations to spreadsheets are typically the ability to import and use very large data sets, as most spreadsheets have record or field-size limitations. Further, more complex analysis and the merging of data sets is more challenging in a spreadsheet application.

Internal audit departments that rely heavily on spreadsheets must be careful when backing up queries and data analytics. Because spreadsheet applications and the data often reside on the computers of the individual auditors, there is a risk that data could be lost or corrupted if something happens to the auditor or their computer. Care should be taken and procedures should be established to ensure data, queries, and results are housed in a separate, secure location.

Specialized data analysis tools

An internal audit department looking to move beyond the capabilities of spreadsheet applications to perform data analytics should consider the acquisition of specialized data analytics tools. In addition to generic research data tools, several applications have been designed and developed specifically for use by internal auditors.

Specialized internal audit data analytics tools have several advantages over basic spreadsheet applications. These tools typically do not have file size limitations, although auditors must be cognizant that they are always limited by the size and capabilities of the hardware that they are utilizing. Further, specialized tools are designed to more readily assist auditors in merging and comparing data sets, as well as performing complex data analytics.

Most modern analytics tools can interface with the organisation's systems. When this is done, data can be brought directly into the system on a real-time basis or on a set periodic schedule. The obvious advantage is that data does not have to be extracted for each usage. This capability allows auditors to establish continuous auditing techniques whereby analysis is automatically performed and outputs are provided to auditors using pre-established criteria.

Before deciding to integrate data analytics applications, CAEs should work with their IT professionals to ensure that systems are properly tested in the organisation's environment and will be properly supported within the IT architecture. Finally, the CAE must ensure that hardware investments are made to properly support the acquired tools.

Visualization

In recent years, a growing trend has emerged in the use of visualization tools to assist in data analytics. Visualization tools take the underlying data and present it to the user, whether it is internal auditors or stakeholders, in a format that is easier to digest.

By viewing data in chart and other forms, and providing drill-down capabilities, the capacity to perform iterative analysis is enhanced. Auditors and stakeholders can visually see exceptions, drill down into them, update analytics, and perform additional analytics.

Further, internal auditors who employ visualization tools can perform dynamic presentations. Rather than showing results to stakeholders with static charts and graphics, auditors can present interactive information that allows stakeholders to drill down into data and/or modify analytics in real time.

Like other specialized technologies, visualization tools require an investment to both acquire licenses and also to ensure that users are trained properly. CAEs should ensure that their department is well versed in performing data analytics before moving to more complex tools.

Progress through sharing

CAEs and other professionals looking to develop a data-driven methodology, implement use of a new application, or enhance their departmental capabilities should consult with peers. While peers in other organisations cannot share specific results of data analytics, consultations on approaches to both mature the organisation and implement data analytics is typically not proprietary.

Most software companies that sell data analytics software provide free customer support designed to ensure success. Potentially even more valuable, the software companies support user communities that provide on-demand resources as well as seminars and conferences where users gather and share leading practices.

It is advisable before spending any time or money, CAEs and their management teams consult with peer organisations to ensure investments are made in the tools that will best suit their department's needs.

CLOSING THOUGHTS

Increase your capacity

Invest in people and technology

Organisations globally, regardless of size, complexity, industry, or regulatory environment, are increasingly using data to make strategic and tactical business decisions every single day. Internal auditors have that same ability to improve the effectiveness and efficiency of their work using data analytics. According to the 2018 IIA Pulse of the Profession survey, 62 percent of the 636 CAEs and directors who responded have fully or partially implemented data analytics, with an additional 27 percent planning to implement.

A data-driven internal audit methodology increases the capacity of internal audit to provide assurance and value-added services. According to a 2017 Grant Thornton survey, 60 percent of internal audit survey participants enjoy moderate or major benefits from data analytics. Amongst those participants that saw benefits, they noted:

- More transactions are reviewed/ monitored in less time (51 percent).
- Added assurance is taken from the work performed (46 percent).
- Fraudulent transactions are identified more quickly (29 percent).

However, the investment required in resources, both human and technology, can be significant. CAEs must develop a game plan to drive greater uses of data in their departments and leverage the lessons learned of their peers and colleagues.

About The IIA

Established in 1941, The IIA is an international professional association with global headquarters in Lake Mary, Fla., USA. The IIA is the internal audit profession's international standard-setter, sole provider of globally accepted certifications, and principal researcher and educator.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends that you always seek independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org