GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

IPPF – Practice Guide

Data Analysis Technologies

The Institute of Internal Auditors

Unhappy with your current audit software?
Still using a spreadsheet for audit analysis?

It's time to take a closer look at

IDEA

Global Technology Audit Guide (GTAG®) 16
Data Analysis Technologies

Authors:

Altus J. Lambrechts, CISA, CRISC

Jacques E. Lourens, CIA, CISA, CGEIT, CRISC

Peter B. Millar

Donald E. Sparks, CIA, CISA

August 2011

1. Executive Summary

Change can be difficult for anyone. Inventor Charles Kettering once said, "The world hates change, yet it is the only thing that has brought progress." This adage is particularly true when it comes to moving beyond the tried and true methods of manual auditing towards computer assisted audit techniques (CAATs) and the use of data analysis.

Although internal auditors have been doing data analysis for more than 25 years, it has only recently started to become standard practice. By our nature, most accountants and auditors are inclined to stick with what has worked in the past, rather than reach outside our comfort zones for an alternative that could help us accomplish more. What we should be asking ourselves is, "Could we do something electronically in 20 minutes that would normally take us 20 hours, and possibly improve the quality of our work as a result?"

Because all organizations are impacted by IT in various forms, it is nearly impossible to conduct an effective audit without using technology. Current audit standards already require consideration of the use of data analysis for good reason. The use of data analysis allows auditors to view high-level organizational operations and drill down into the data. It can be used throughout all phases of an audit. It also can be used to identify errors, which may lead to the discovery of fraudulent activity. While technology may be used to improve the audit and reduce the time necessary to complete the engagement, some auditors may still be reluctant to make the switch.

While data analysis could theoretically be performed manually, it is most effective when implemented using data analysis technology. It is important for chief audit executives (CAEs) and their staff to realize that the use of data analysis technology is not limited to the scope and activities associated with IT audit alone. The use of technology-based audit techniques in general and data analysis technology in particular is far more widespread. The IIA defines technology-based audit techniques as, "Any automated audit tool, such as generalized audit software, test data generators, computerized audit programs, specialized audit utilities, and CAATs."[1] Owing to the broad scope of this definition, the focus of this GTAG is on data analysis technologies. The use of data analysis technology is part of the bigger technology armor that assists auditors in increasing audit coverage, performing more thorough and consistent audits, and ultimately increasing the levels of assurance that they provide their organizations.

This guide aims to help CAEs understand how to move beyond the tried and true methods of manual auditing toward improved data analysis using technology. After reading this guide you will:

- Understand why data analysis is significant to your organization.

- Know how to provide assurance more efficiently with the use of data analysis technology.

- Be familiar with the challenges and risks that you will face when implementing data analysis technology within your department.

- Know how to incorporate data analysis at your organization through adequate planning and appropriate resource structures.

- Recognize opportunities, trends, and advantages of making use of data analysis technology.

To further assist CAEs and other individuals who use this guide, we also have included a detailed example of the application of data analytics to procurement control activities in Appendix A. Consistent with where most data analysis starts, these examples are largely focused on simple data matching and reperformance of automated system functionality used in providing assurance.

---

[1] www.theiia.org/guidance/standards-and-guidance/ippf/standards/glossary

2. Introduction

Data analysis as used by internal auditors is the process of identifying, gathering, validating, analyzing, and interpreting various forms of data within an organization to further the purpose and mission of internal auditing. Data analysis is typically used throughout the execution of assessment activities as well as providing other value-added consulting activities.

Data analysis technologies are computer programs the auditor uses as part of the audit to process data of audit significance to improve the effectiveness and efficiency of the audit process. When data analysis is being used, the overall objective and scope of an audit does not change. Data analysis must be seen as another tool that can be used to achieve the objective of the specific audit.

Data analysis tools may consist of packaged, purpose-written utility programs or system management programs. Different technologies fall under this concept, including database interrogation tools (generic standard query language–based tools) and audit-specific packages.

Opportunities

In today's economic environment many companies are striving to reduce costs. Together with new audit standards, this provides internal audit departments with an opportunity to make use of data analysis and makes the concept "do more with less" a potential reality.

Data analysis also can be an enabling technology that assists audit departments in fulfilling their responsibilities to evaluate and improve the governance, risk management, and control (GRC) processes as part of the assurance function. Data analysis gives audit departments the ability to conduct assessments on the operating effectiveness of internal controls and to look for indicators of emerging risk. The use of data analysis throughout the audit cycle is discussed later in this section.

In the days when mainframe computers ruled the business world, only the best funded internal audit functions could even consider moving data analysis activities into the department. Over the past decade, technology has advanced at a great speed, resulting in price reductions that have made it easier to implement data analysis within an organization. Through this, audit analytics have evolved from specialized technology that was once the domain of specialized IT auditors into an essential technique that has a valuable role to play in the majority of audit procedures. Many audit functions now aim to integrate audit analytics throughout the audit process and expect all auditors to have an appropriate level of technological competency.

There are many benefits that may be realized from the use of data analysis, including:

- **Productivity and cost savings**
  Data analysis technology has enabled a number of organizations to realize significant productivity improvements in audit planning, risk assessment, and increasing the breadth and depth of audit coverage during the engagement. Ultimately, this has enabled audit departments to broaden the scope of their assurance activities, without having to increase audit staff. In some circumstances, automation of analytic steps has lead to cost savings through the reduction of staff necessary to complete the audit plan.

- **Efficiency in data access**
  Data analysis technologies enable auditors to access and query data by themselves, thereby decreasing their reliance on busy IT personnel having to run data extracts. This helps provide a higher degree of confidence in the accuracy and completeness

---

Related Standards/Guidance

Standard 2300: Performing the Engagement

■ Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.

Standard 2310: Identifying Information

■ Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

Standard 2320: Analysis and Evaluation

■ Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.

Practice Advisory 2320-1: Analytical Procedures

■ Internal auditors may use analytical procedures to obtain audit evidence. Analytical procedures involve studying and comparing relationships among both financial and nonfinancial information. The application of analytical procedures is based on the premise that, in the absence of known conditions to the contrary, relationships among information may reasonably be expected to exist and continue. Examples of contrary conditions include unusual or nonrecurring transactions or events; accounting, organizational, operational, environmental, and technological changes; inefficiencies; ineffectiveness; errors; fraud; or illegal acts.

of the data population being analyzed and introduces efficiencies in verifying the accuracy of that information.

- **Audit risk**
  The use of data analysis can significantly reduce audit risk by honing the risk assessment and stratifying the population.

Trends

There is increasing pressure on audit departments to do more with less. Internal audit's role is at the forefront as the profession looks to provide more assurance and transparency to the audit committee and senior management around everyday organizational activities. To accomplish this, the current focus of many audit teams is to enhance the quality of their work and effectiveness of the department using technology. They need to be more productive and better focused on emerging risks. Audit teams also are seeking to deliver timely value to the enterprise by distributing, tracking, and escalating potential issues for better organizational insight and control.[2]

---

[2] IIA Global Audit Information Network (GAIN) 2009 IT Audit Benchmarking Survey.

3. How Can Data Analysis Help Internal Auditors?

Data Analysis can help internal auditors meet their auditing objectives. By analyzing data within key organizational processes, internal audit is able to detect changes or vulnerabilities in organizational processes and potential weaknesses that could expose the organization to undue or unplanned risk. This helps identify emerging risk and target audit resources to effectively safeguard the organization from excessive risk and improve overall performance. This also enables internal audit to identify changes in organizational processes and ensure that it is auditing today's risks — not yesterday's.

By analyzing data from a variety of sources against control parameters, business rules, and policies, internal audit can provide fact-based assessments of how well automated controls are operating. Data analysis technology also can be used to determine if semi-automated or manual controls are being followed by seeking indicators in the data. By analyzing 100 percent of relevant transactions and comparing data from diverse sources, internal audit can identify instances of fraud, errors, inefficiencies, or noncompliance.

A number of specific analytical techniques have been proven highly effective in analyzing data for audit purposes.

- Calculation of statistical parameters (e.g., averages, standard deviations, highest and lowest values) to identify outlying transactions.

- Classification to find patterns and associations among groups of data elements.

- Stratification of numeric values to identify unusual (i.e., excessively high or low) values.

- Digital analysis using Benford's Law to identify statistically unlikely occurrences of specific digits in naturally occurring data sets.

- Joining different data sources to identify inappropriately matching values such as names, addresses, and account numbers in disparate systems.

- Duplicate testing to identify simple and/or complex duplications of organizational transactions such as payments, payroll, claims, or expense report line items.

- Gap testing to identify missing numbers in sequential data.

- Summing of numeric values to check control totals that may have errors.

- Validating data entry dates to identify postings or data entry times that are inappropriate or suspicious.

Benford's law definition

- Benford's Law gives the expected frequencies of the digits in tabulated data. The set of expected digit frequencies is named after Frank Benford, a physicist who published the seminal paper on the topic (Benford, 1938). Benford found that contrary to intuition, the digits in tabulated data are not all equally likely and have a biased skewness in favor of the lower digits.

- Benford begins his paper by noting that the first few pages of a book of common logarithms show more wear than the last few pages. From this he concludes that the first few pages are used more often than the last few pages. The first few pages of the logarithm books give us the logs of numbers with low first digits (e.g., 1, 2, and 3). He hypothesized that the first pages were worn because the most "used" numbers in the world had a low first digit. The first digit is the leftmost digit in a number (for example, the first digit of 110,364 is a 1). Zero is inadmissible as a first digit and there are nine possible first digits (1, 2, . . . , 9). The signs of negative numbers are ignored and so the first two digits of 34.83 are 34.

- Benford's results showed that, on average, 30.6 percent of the numbers had a first digit 1, and 18.5 percent of the numbers had a first digit 2. This means that 49.1 percent of his records had a first digit that was either a 1 or a 2. At the other end of the "digit-scale" only 4.7 percent of his records had a first digit 9. Benford then saw a pattern to his results. Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations (Wiley Corporate F&A) Mark Nigrini (Author)

Data analysis can be used throughout a typical audit cycle. While individual audit cycle definitions and steps may vary, the following breakdown provides some of the ways data analysis can be employed during various stages in an audit cycle.

Planning

Data analysis can be greatly effective in identifying data-driven indicators of risk or emerging risk in an organization.

This can help internal audit define and create an audit plan that focuses on the areas of highest concern. The internal audit activity should consider prioritizing the use of data analysis for risk assessment during the audit planning stage, where the data is available, and where this approach is applicable.

Data analysis technology can be effectively employed to identify indicators of risk in a variety of processes. Consider the following examples:

- Revenue by location, division, or product line.

- Revenue backlogs by value and age.

- Personnel changes in key positions (legal, finance, research & development).

- Volume of manual journal entries or credit notes.

- Aging accounts receivable balances or inventory levels.

- Vendor management (number of vendors, volume of transactions).

- Procurement card vs. purchase order procurement.

- Average days for customer payment.

- Industry code of supplier on credit card purchases.

Preparation

Data access and preparation can be a challenging step within the audit process. Requests to IT departments can take weeks and the resulting data can often be incomplete or incorrect, making for an inefficient process. By using data analysis technology during the audit preparation phase, many of these delays can be avoided. Auditors skilled in the use of data analysis can source the data required for the audit engagement, do data integrity and validity checks, and prepare test routines for staff auditors to use once the audit commences. This will provide audit teams with streamlined access to reliable data sets or even automated access to multiple data sources to allow for quick and efficient analysis of data. Data should be housed in a centralized repository allowing the audit team to analyze data sets according to their authorization and need for access.

Testing

A great deal of audit testing uses organizational data to some extent — often to a significant extent. Due to ever increasing amounts of data, some auditors have relied on techniques such as sampling or spot checks. These techniques may be ineffective at uncovering anomalies and indicators of failed or inefficient internal controls. To improve effectiveness in the search for errors and unusual transactions, audit teams can use data analysis technology to analyze entire data populations. Once initial analysis is done, efforts can be focused on areas where exceptions were found, making more efficient use of audit resources. The ability to automate repetitive tests by using analytic scripts increases overall departmental efficiency and allows for greater insight into high risk areas. Results and scripts should be stored in a centralized repository allowing audit team members to review findings and access and re-use analytic procedures.

Review

The analytic routines and the results they generate should be included in the audit review. This helps ensure that the conclusions drawn from using data analysis can be relied on and that any mistakes in the query are identified and corrected or that conclusions that were drawn from those results are not erroneous.

4. Using Data Analysis Technology

4.1 Data Analysis Software Tools

Leading internal audit activities have a lot in common when looking for data analysis tools. They look for data analysis tools (i.e., software) that are easy to learn and can realistically be used by the entire audit staff, not just a select few. The software must measurably improve audit techniques and shorten audit cycles right out of the box. Investments in time and skills to develop analysis routines created during one audit can be used again on the same or similar audits leading the function forward into continuous audit/monitoring processes.

Purpose-built data analytic technologies for audit have been around for over 20 years. Yet according to the PricewaterhouseCoopers 2010 State of the Internal Audit Profession Study, auditors for the most part are not taking advantage of them effectively. The following chart illustrates the areas in which data analysis technologies are being used most frequently.[3]

When the right software is implemented, the results can be significant. Successful internal audit functions have stakeholders that recognize the efficiencies in audit processes and appreciate audit results that regularly disclose previously unknown issues. And just as important, internal audit leaders know and are confident the audit tests being conducted are done in a manner consistent with their directions. And while they may not roll out the software to 100 percent of the staff initially, in a few short months many staff would be able to perform data analysis.
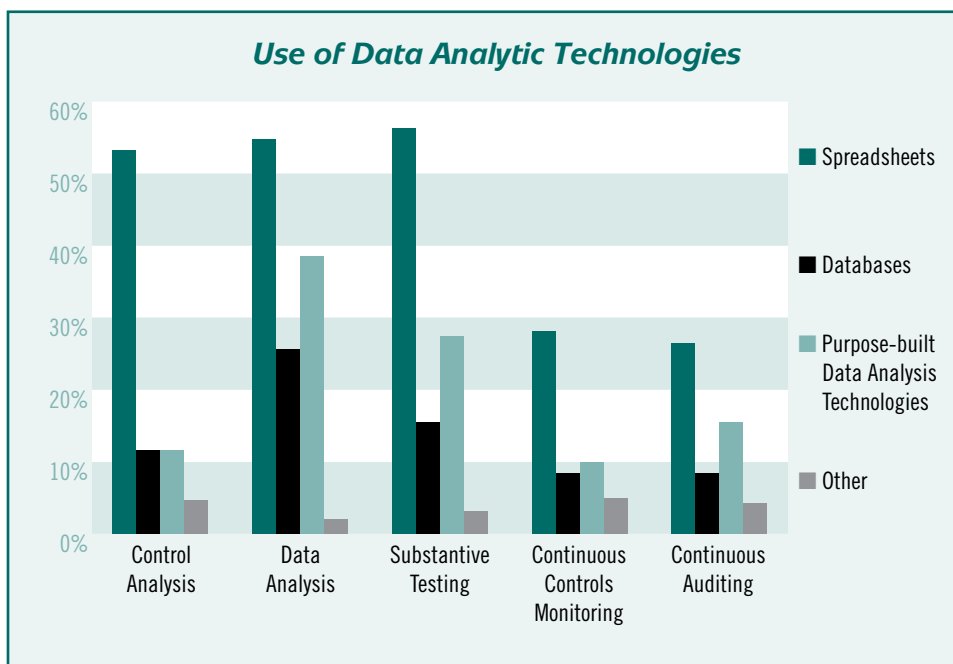
As with the adoption of any software tool or technology, initial product acquisition cost should be considered, in addition to ongoing maintenance and support costs for the technology(s) selected. A needs assessment should be carried out to ensure that the technology(s) selected are appropriate for the intended usage — ranging from ad hoc, mobile use to centralized processing of large volumes of data. This should take into consideration not only the immediate needs being addressed, but also what capability levels are envisioned for the future. This needs assessment may result in hardware acquisition costs for laptop computers, centralized server hardware, or additional data storage capacity.

The use of data analysis technologies also requires the support and commitment of an organization's IT department. The CAE should engage in planning with IT resources up front to highlight the overall data analysis strategy, sought after benefits, and data access requirements of the audit department. Data access protocols should be established up front, and any risks identified relating to the access, sharing, and storage of sensitive data should be addressed. This may entail the implementation of centralized data analysis capabilities, where client/server architecture is implemented, or the need for data encryption and protection software to safeguard the organization from data loss.

Appendix B has an example ranking matrix that can be used to help evaluate various software options for use in data analysis.

4.2 Auditor Skill Sets

In deciding to implement data analysis within an audit department, the CAE needs to consider the skill sets that exist within their department. For some, the concepts involved in accessing and working with data are beyond their experience or comfort level. The

Use of Data Analytic Technologies

(Bar chart showing percentage use across categories: Control Analysis, Data Analysis, Substantive Testing, Continuous Controls Monitoring, Continuous Auditing — for Spreadsheets, Databases, Purpose-built Data Analysis Technologies, and Other.)

---

[3] Adapted from: A future rich in opportunity: Internal audit must seize opportunities to enhance its relevancy PricewaterhouseCoopers 2010 State of the Internal Audit Profession Study, March 2010, p.22.

Attributes of Data Analysis Software for Audit

- Able to analyze entire data populations covering the scope of the audit engagement.

- Makes data imports easy to accomplish and preserves data integrity.

- Allows for accessing, joining, relating, and comparing data from multiple sources.

- Provides commands and functions that support the scope and type of analysis needed in audit procedures.

- Generates an audit trail of analysis conducted that is maintained to facilitate peer review and the context of the audit findings.

- Supports centralized access, processing, and management of data analysis.

- Requires minimum IT support for data access or analysis to ensure auditor independence.

- Provides the ability to automate audit tasks to increase audit efficiency, repeatability, and support for continuous auditing.

CAE needs to determine if an investment in training of existing personnel is needed, or if hiring of new staff with data analysis expertise is more appropriate. In either case, some degree of training and professional development will most likely be required. This should be budgeted for in terms of both time and money as an ongoing cost to ensure the long-term success of their data analysis implementation.

4.3 Potential Barriers

While the benefits of using data analysis technology are generally well known, adoption rates show that there are a number of barriers to overcome before more widespread use of data analysis can occur. The CAE should be cognizant of these barriers and address them to realize the gains data analysis technology enables. The barriers include:

- **Poorly defined scope.** Once audit objectives are determined, the scope of the intended use of data analytics should be understood before starting the analysis. Some internal auditors tend to jump into the analysis without any scope expectations and then try to make sense of the data. However, not understanding the scope can lead to results that contribute little value or are irrelevant.

- **Data location and access.** Knowing what data to find and where, as well as ensuring access to the right data (e.g., data source files rather than altered metadata or extracts) before performing the data analysis, can save internal auditors valuable time. In addition, having access to the right data at the right time can help achieve relevant and timely results. There are three considerations: the volume of data required; the variety of data types, formats, and sources; and the veracity and accuracy of the data sets.

- **Data understanding.** If the auditor does not understand the data to be analyzed (the data's source, context, use, and meaning) faulty conclusions can be reached, regardless of the sophistication of the analysis technique.

- **Data preparation.** Cleaning and preparing the data is important, especially when importing data from different source files. Consequently, internal auditors need to spend time normalizing and aggregating the information to make sure the format is consistent for all data, thus helping to ensure the accuracy of results.

- **Manually maintained data.** Using data that has been maintained manually can pose problems pertaining to data integrity as change controls might be lacking or ineffective. Whenever possible, internal auditors should use automated data as the basis for the analysis and verify it against existing manually maintained data.

The benefits of using data analysis are many, however, the items above should be considered by the CAE in implementing and executing an effective data analysis strategy. Many of these challenges and risks can be addressed through professional development of audit staff, modification of audit procedures, and the technology selected for audit's use. For further guidance on how to provide assurance around the use of data analysis technologies and other user-developed applications, please refer to *GTAG 14: Auditing User-developed Applications.*

5. Elaboration on Key Technology Concepts

5.1 Technology Used for Data Analysis

Internal audit activities can choose either general purpose, readily available tools such as spreadsheets, or look to purpose-built technologies for analyzing data. The manifest advantage of data analysis technology is that it addresses the specific needs of the auditor when analyzing data to evaluate the operating effectiveness of internal controls, adherence to specific compliance requirements, assessing organizational risk, and detecting indicators of fraudulent activity. For additional guidance related to fraud detection, see The IIA's Practice Guide, Internal Auditing and Fraud and GTAG 13: Fraud Prevention and Detection in an Automated World.

When evaluating a data analysis technology for auditing, there are a number of essential attributes that should be considered. These may be divided into three areas:

- Data access.
- Audit-specific capabilities.
- Logging and automation.

5.1.1 Data Access

Simply accessing the data required for an audit can be a daunting task. This is due, in part, to the amount of time it can take to receive data extracts from busy IT departments. Under pressure to do more in less time and with fewer resources, auditors are looking to eliminate obstacles and streamline audit processes. An effective data analysis technology enables auditors by providing them with direct data access either by "pulling" data on demand or by scheduled data "push" techniques for regular data feeds in support of continuous auditing or repetitive testing of specific data sets. This has the joint benefit of streamlining the overall audit process and relieving busy IT staff from repeated data requests by the audit function.

There are three additional data access challenges that need to be overcome to assist audit's use of data analysis tools:

- The volume of data required to provide effective assurance of organizational processes.
- The variety of data types, formats, and sources.
- The veracity or truthfulness and accuracy of the data sets.

Volume

An effective data analysis technology for internal audit must be able to analyze entire data populations to ensure that the entire picture is visible. Analysis of entire data populations allows for unprecedented insight into organizational operations. Suspicious transactions may be detected sooner and corrective action initiated before problems escalate, become material weaknesses, or require external reporting.

In recent years, data volumes have grown to the extent that there may be too much data to consider downloading or importing to a PC for analysis. An effective data analysis solution in today's environment likely needs to incorporate server-based platform solutions that provide a robust and dependable technical architecture that preserves both the integrity and controlled access to data. In such a solution, data can be analyzed by the auditor within the secure IT environment, thereby reducing network traffic and minimizing the risks involved in converting, duplicating, and disseminating sensitive organizational data.

Variety

Most organizations rely on several applications that run on a variety of operating systems, collecting data in a variety of formats or databases. While generalized data analysis software has become more adept at importing data, they still fall short of being able to deal with data from different formats and operating environments. The risk is the inadvertent modification of the data during the conversion process. For instance, mainframe data is usually in extended binary coded decimal interchange code format and cannot be read by a PC-based spreadsheet without conversion.

An effective data analysis solution for audit needs to be able to read and compare a broad variety of data formats including relational data, legacy data, spreadsheets, report files, flat files, extensible markup language, and eXtensible business reporting language-formatted data. Where data resides in databases, an effective technology needs to be able to access this data quickly and efficiently to meet internal audit's needs.

Veracity

Veracity, or the truthfulness or accuracy of data, is paramount in the audit process. An effective data analysis technology for audit purposes must protect the integrity and quality of data. With data extracts and format conversions, the integrity of data can be inadvertently compromised and introduce unintended audit risk into the process. An effective data analysis technology must be able to access and analyze data without altering it or subjecting it to accidental change.

Effective data analysis tools for audit need to protect the user from accidentally changing values and the integrity of the records in the data set. It must preserve the veracity of the data to prevent the skewing of analytical results, which could lead to material errors in findings and erroneous audit recommendations.

While the selected data analysis technology should protect the integrity and quality of the source data from alteration, often the source data itself has inherent data quality errors

or deficiencies. When using data analysis, auditors should always check the data for validity errors. Getting the correct and complete data is a prerequisite of effective data analysis. For instance, do the numeric fields in the source data contain valid numbers — or are characters present in this field or are there blank entries? Do key fields, such as social security or social insurance numbers, contain valid entries? Does the data contain records within the expected date range or is it under- or overrepresented in the data set? When source data errors are identified, data extracts should be repeated to get the expected data range, data cleansing activities should be conducted to correct faulty data fields, or "bad data" should be isolated from the main analysis and subsequently investigated to see if it substantially impacts the overall assessment of the audit.

5.1.2 Audit-specific Capabilities

Data analysis technology for internal audit's use needs to have the features and functionality that auditors require to do their job effectively. Not only should it deal with the data access challenges, but it also needs to support the way in which auditors work and the types of analytics that are appropriate to the audit task.

Some aspects of data analysis involve assessing the integrity of organizational processes and practices, evaluating the efficacy of controls, conducting risk assessments, and, in some cases, fraud detection. Invariably this means that data must be analyzed from a diversity of sources to seek patterns and relationships. Auditors need to organize their view of the company data in a way that suits the audit objectives.

This view gives users the ability to set an appropriate context from which to compare and contrast data from diverse sources. For example, if part of an audit process is fraud detection, data analysis may be used to great effectiveness. One might compare an employee master file with an approved vendor database. If there is a match between an employee's address and the address of a vendor, it might indicate the presence of a "phantom vendor" and that an employee is attempting to perpetrate fraud. In such a case,

the auditor needs to have a data analysis tool that allows them to visually present these data files in relationship to one another.

When using data analysis, auditors need to compare and contrast diverse sources of information, validate data integrity and accuracy, and look for patterns and anomalies in data. The audit process may need to support assertions inherent in published financial statements such as completeness, accuracy, occurrence, valuation, and presentation. Data analysis software may have algorithms designed to perform these tests without having to program custom queries or macros to reduce the audit risk in user developed applications (UDAs). For additional guidance related to UDAs, see GTAG 14: Auditing User-developed Applications.

Purpose-built data analysis software will have commands and functions that look for duplicates; detect gaps in numeric sequences; and group transactions by type, numeric range, and age. The ability to filter vast amounts of data quickly and efficiently also is a key requirement. Advanced pattern detection techniques, such as digital analysis, are extremely helpful when seeking anomalies in data.

When comparative analysis is required, the technology needs the ability to merge data files (often from different sources and in different formats) and look for matched or unmatched records. For tasks requiring the comparison of data from numerous sources, the ability to relate diverse data sets together also may be necessary. Because the audit process often involves retrospective analysis of vast amounts of data, an effective data analysis technology needs highly efficient read algorithms to process millions of records rapidly. These algorithms must be powerful and reliable to perform tasks either quickly in interactive data analysis or for sustained periods of time in lengthy and complex automated analysis. Depending on the nature of the audit work being done, this interactive work can be ad hoc for planning, initial scoping, or investigative work. It also can be scripted for repetitive analysis of organizational processes from period to period, such as quarterly reviews of key controls. In organizations that want to implement a continuous auditing methodology,

Data analysis tasks can be grouped into three types:

Ad Hoc	Repetitive	Continuous
Explorative and investigative in nature.	Periodic analysis of processes from multiple data sources.	"Always on" — scripted auditing and monitoring of key processes.
Seeking documented conclusions and recommendations.	Seeking to improve the efficiency, consistency, and quality of audits.	Seeking timely notification of trends, patterns and exceptions. Supporting risk assessment and enabling audit efficiency.
Specific analytic queries — performed at a point in time — for the purpose of generating audit report findings.	Managed analytics — created by specialists — and deployed from a centralized, secure environment, accessible to all appropriate staff.	Continual execution of automated audit tests to identify errors, anomalies, patterns and exceptions as they occur.

the data analysis technology selected must be able to support the scheduling and automation of data analysis tests.

An example of an ad hoc analysis could be 'suspicious vendor' and 'phantom employee' analysis for acquisition due diligence. An audit team member could generate a few specific queries comparing vendors to employees to see if there is a match. If there is, this may be an area warranting deeper analysis. Ad hoc is often explorative and investigative in nature and helps target high-risk areas for more involved analysis.

A repetitive analysis example could be a quarterly journal entry analysis. Data analysis can be used to help validate the operating effectiveness of controls in this area and identify control failures — even in manual controls. For instance, data analysis can be used to identify:

- Journal entries by unauthorized or restricted users.

- Duplicate journal entries.

- Invalid account postings.

- Journal entries pre- and post-period close.

- Frequently reversed journal entries.

An example of continuous analysis could be a pay cycle review in a high transaction environment with the need for weekly reporting to a third-party recovery partner. In this case, there is a need to provide continuous reports and identify exceptions and gaps via user-defined parameters in line with internal controls.

5.1.3 Logging and Automation

One of the keys to improving audit performance and driving better results is the ability to automatically record what has been done and reliably repeat it in subsequent areas or audits. It is for this reason that more effective data analysis technologies automatically generate comprehensive audit trails. They also provide for reliable task automation, from accessing the data at source, to verifying its validity, to performing the detailed analysis, and generating audit reports.

There are a number of attributes that constitute an effective audit trail. An effective audit trail is one that records all of the commands run by the application, status messages that provide insight into command execution, and any results generated by the actions of the user. This provides a number of critical artifacts for an effective audit, including a context for the audit findings.

The audit trail documents the steps taken to uncover exceptions that can now be explained, substantiated, and defended where necessary. The audit trail also provides a mechanism for peer or supervisory review. Review of audit steps is an important activity to ensure the accuracy, completeness, and quality of the audit process. This review demonstrates to audit management that opinions expressed in audit reports are accurate and that the audit recommendations are sound.

A final benefit of an audit trail is the ability to recall previous results. An audit trail records not only the commands and functions used to identify exceptions and anomalies, but also intermediary and final results. In this way, auditors may compare past findings with current findings to see if the recommendations have been acted upon, or if there is a substantive shift in the behavior of the organization that may be an indicator of emerging risk.

If meaningful results or insight are achieved through a data analysis process during an audit, they are probably worth repeating again in the future. An effective technology enables simple and straightforward task automation. Effective technologies provide for a variety of ways to automate analytical tasks either through a "task recorder" functionality or through the selection of commands recorded in the audit trail.

It is through task automation that auditors themselves may create batteries of tests to streamline the overall audit process and contribute to the aspects of continuous auditing involving the recurring analysis of data to identify indicators of failed controls, noncompliance, and fraudulent activity.

5.2 The Link Between Data Analysis and Continuous Auditing

The use of data analysis can span a diversity of needs and approaches, and allows for efficient analysis across this continuum.

There has been much written and discussed in recent years about the increasing expectations placed on internal auditing and the importance of technology — specifically data analysis, continuous auditing, and monitoring — to help internal audit and management achieve their respective goals.

The effective use of data analysis technology is a precursor for continuous auditing. Competency in understanding key business processes and being able to analyze and interpret the data that reflects those activities is a requirement. Likewise, internal audit departments need to develop increasing levels of sophistication in using data analysis if they are to implement a technology-enabled continuous auditing methodology. The CAE should be able to assess the levels of sophistication or capability within their department to ensure that it aligns with their departmental goals. For the purposes of this GTAG, five capability levels are discussed.

Level 1 – Basic Use of Data Analysis

This level is characterized by the basic use of data analysis technology to perform queries and analyze data in support of a specific audit objective. Activities typically include statistical analysis, classifications, or summarization of data. Usage

is usually ad hoc by a limited number of audit staff and may be unplanned.

This use of data analysis helps auditors rapidly gain insight into risk and control issues in a given audit area. However, there is room for improvement. The use of data analysis technology can be better integrated into audit procedures and at different stages in the audit cycle. This requires an investment in changing audit processes — educating audit staff in the concepts of data analysis and the technology itself.

Level 2 – Applied Analytics

Usage at this level builds on the basic level and is characterized by data analysis being fully integrated into targeted audit processes. Both audit planning and the design of an audit program take data analysis into account — effectively creating a "data analysis-enabled audit program." Within this more structured approach to using data analysis, comprehensive suites of tests may be created, reviewed, and subject to quality assurance procedures. Usage is often progressive, with additional tests being added over the course of time and during each repetition of an audit process.

At this stage, data analysis begins to transform the audit process, providing substantial improvements in efficiency, levels of assurance, and the overall value of findings. Certain tasks can be performed in a fraction of the time it previously took, thereby enabling audit to focus on areas of new or evolving risk.

Level 3 – Managed Analytics

The Managed level is the logical evolution from the Applied stage. This increased level of sophistication is in response to some of the challenges inherent in a more widespread, decentralized use of data analysis. In this more organized and controlled approach to data analysis, data, audit tests, results, audit procedures, and documentation are housed in a centralized and structured repository. Access to and use of this content is aligned with key audit procedures and is controlled and secure. This makes it more practical for nontechnical audit staff to access and use the results of tests.

Once data analysis is managed centrally, audit teams can benefit by increased efficiency through the sharing of data analysis work (data, tests, and results). Data analysis use is repeatable, sustainable, and easier to maintain the overall quality and consistency of analytic work. It is at this level that the basic building blocks for continuous auditing are in place. One of the key benefits of this level is also that of making the whole process more sustainable by reducing the risks of relying on individual specialists who may leave, taking critical knowledge with them. Analytic procedures at this level are well documented and centralized in a way that makes review by management easier and more efficient.

Level 4 – Automated

Define the term Continuous Auditing.

Solution:

"Continuous auditing is any method used by auditors to perform audit-related activities on a more continuous or continual basis. It is the continuum of activities ranging from continuous controls assessment to continuous risk assessment — all activities on the control-risk continuum. Technology plays a key role in automating the identification of exceptions and/or anomalies, analysis of patterns within digits of key numeric fields, analysis of trends, detailed transaction analysis against cut-offs and thresholds, testing of controls, and the comparison of the process or system over time and/or other similar entities."

~GTAG 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment.

The Automated level builds on the capabilities established to support Managed Analytics. The building blocks established at the previous levels form the basis for increased automation of analytic processes and, where appropriate, the implementation of continuous auditing. Data access protocols have been established for the automated running of analytic tests. Comprehensive suites of tests have been developed, tested, and are available in a central, controlled environment.

However, continuous auditing requires more than addressing technology issues. It requires a significant shift in audit processes compared to traditional auditing methods. Most internal audit departments commence continuous auditing in one area and then expand to additional areas over time as appropriate procedures are established. The result of the use of automation is that it becomes possible to perform concurrent, ongoing auditing of multiple areas.[4]

While effective continuous auditing provides clear benefits in terms of audit productivity and effectiveness, there remains a risk that findings are not communicated to management or are not acted on in a timely manner by management to add value to the business through improved controls and business performance. When implementing a continuous auditing

---

[4] For additional information on continuous auditing, please refer to GTAG 3: *Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment.*

approach, processes need to be put in place to ensure that findings are communicated to management effectively and procedures are put in place to ensure that the issues identified are being acted on.

Level 5 – Continuous Monitoring

Once a continuous auditing program has been established, with internal audit regularly producing reports on control problems and potential instances of error, fraud, or compliance failures, then the logical next step is to have management take over the monitoring of their own processes.

Internal audit is often in the best position to demonstrate to management the value of data analysis in detecting control problems and improving operational performance. By encouraging and supporting the implementation of continuous monitoring, the benefits of data analysis techniques become evident to a wider audience and start to become applied more broadly. The ability to identify and quickly resolve exceptions such as fraud, error, and abuse has a clear value and can provide a quantified benefit to the organization.

Continuous monitoring also can become an important component within an organization's risk management processes, helping to provide business with a clearer picture of risk issues and trends.

In general, the view of the internal audit profession is that management is responsible for continuous monitoring and internal audit should independently assess the impact of those activities. Using this approach, the desired outcome can be a combination of continuous auditing performed by internal audit and continuous monitoring performed by management, which together provide continuous assurance over the transactional integrity and the effectiveness of controls.

Benefits of CM and CA[5]

Continuous monitoring can enable an enterprise to:

- Increase value through improved financial and operating controls
- Accelerate reporting to support more rapid decision making and business improvement
- Detect exceptions in real time to enable real-time responses
- Reduce – and ultimately minimize – ongoing compliance costs
- Replace manual preventative controls with automated detective controls
- Establish a more automated, risk-based control environment with lower labor costs
- Heighten competitive advantage and increase value to stakeholders

Continuous auditing can enable an enterprise to:

- Improve risk and control assurance, usually in the same or less time than previous approaches
- Reduce costs, including internal audit costs and costs associated with unaddressed control deficiencies
- Increase the level of risk mitigation for business risks
- Achieve a more robust, more effective auditing process
- Expand internal audit coverage with minimal (or no) incremental cost
- Shorten audit cycles
- Identify control issues in real time

[5] *Continuous monitoring and continuous auditing: From idea to implementation*, © 2010 Deloitte Development LLC

6. Where Should Internal Auditors Begin?

A reality of today's highly automated world is that almost every auditor must analyze data. What was once considered a special expertise, a job for IT auditors, or a task that was easily outsourced to another department or organization, has become a core competency for the profession of internal auditing.

Internal audit leadership can start the process by first assessing the strategic goals of the data analysis activities of their function. There are many software products on the market that will catch the attention of staff. Proceeding without first establishing what the function needs to achieve and how to achieve it can cause the process to fail.

Internal Audit Leader Strategies for Data Analysis Clarified

Defining and executing a strategic plan supported by and aligned with management and the audit committee is a good place to begin. Depending on the starting point, this may require internal audit leaders to take a hard look at all aspects of their scope, people, processes, and technologies, and really explore whether or not they have the right strategy and capabilities in place. It is hard to bring about significant change without a plan. Internal audit organizations that break down their vision and goals into key initiatives that can be tackled logically and systematically also are the ones most likely to succeed in driving value in their organizations.

While this GTAG is focused on data analysis technology, it is important to point out that technology alone will not achieve the desired outcomes and benefits articulated herein. For internal audit departments to be successful and achieve rapid and recurring returns on their software investment, three key areas need to be addressed: people, process, and technology.

Without addressing each of these key areas, an effective data analysis program will not be possible.

People

While internal audit departments vary in size and structure, there are certain functions that need to be addressed — either by an individual or several staff members. The larger the department, the greater the degree of specialization can occur.

Training and Education. Internal audit departments need to be educated on the concepts of data, data analysis, and the interpretation of analytical results. With the adage "the truth is in the transactions," auditors can change the way they think about examining organizational processes or compliance requirements. With a deeper understanding of how an organization's activities get recorded electronically in data files and databases, auditors can apply a data-driven methodology to how they evaluate risk, validate the efficacy of internal controls, and identify areas of noncompliance. This also assists how they interpret the results of analysis performed. Are the results indicative of poor internal controls, system deficiencies, poorly trained staff, or indicators of fraud? By understanding data, these determinations can be made and will assist in improving audit performance.

Training also is necessary for the effective use of the technology selected. The internal audit department should establish what their desired end-state of technology use is (i.e., ad hoc use, highly automated audit routines, or implementing continuous auditing). A training regimen needs to be put in place with the outcome in mind to ensure it is achieved according to established project schedules.

Roles and Responsibilities. Auditing is a team activity that requires different roles to ensure effectiveness and quality of work accomplished. In small departments, staff may be responsible for more than one role. CAEs may want to consider establishing specialized roles within their audit teams to effectively deploy data analysis software tools. Some of the key roles could be:

- **Data Specialist** – Member of the audit team or an IT resource assigned to the audit team who has a detailed understanding of the organization's IT infrastructure, data sources, and how to access relevant data to be analyzed. They will understand how to access large volumes from disparate systems, prepare that data for analysis, and make that data available to the team.

- **Data Analysis Specialist** – Member of the internal audit team who is well versed in the detailed use of the technology of choice, and who will perform advanced query and analysis, create and manage automated audit routines, and validate and share results of the analysis across the team.

- **Staff Auditors** – These members of the internal audit team will have a general understanding of data and data analysis software, and will have sufficient competency to review and interpret the results of automated analytic routines and perform simple analysis (sorting, filtering, grouping, and profiling). They also will be trained to document and report on the findings of the analysis performed.

- **Internal Audit Leadership** – The team's leaders should have visibility into what audit steps have been automated or are dependent on the use of data analysis software. This will assist in the oversight of audit activities and overall audit coverage and lets audit leaders review analytic findings across the team and against audit plan objectives.

Process

Integrating data analysis into an audit plan will change the way the audit is conducted, so changing audit processes, procedures, and schedules is necessary. As noted above, data analysis techniques can be utilized throughout an audit cycle, so process changes at each stage need to be considered — not just at the testing phase. In some cases, audit planning and preparation may take longer than normal when using technology as data-driven indicators or when risk or controls weaknesses may affect the audit plan. Where data from multiple sources is deemed required, additional preparation time may be needed to get access to the data. CAEs may want to consider adding access and authorization privileges to their organization's data in their audit charter to streamline this part of the process.

Where the use of data analysis extends to parts of the overall continuous auditing process, significant changes to internal processes will be required to ensure that organizational units are prepared to receive timely notification of exceptions and establish a mechanism of managing those exceptions to close the loop on findings.

Technology

There are a variety of data analysis technologies to choose from. The key is to choose the right technology for your organization's audit tasks, objectives, and IT environment. CAEs should consider what they want to accomplish in the long term and choose the right data analysis technology or suite of technologies to achieve their objectives.

Regardless of what decisions are made with respect to people, processes, or technology, it should be emphasized that internal audit departments should start with a risk assessment that aligns the audit scope with the audit objectives.

Obstacles

Embarking on an increased focus on data analysis using technology will likely have obstacles and challenges. The most common obstacles include underestimating the effort required to implement correctly, lack of sufficient understanding of the data and what it means, and the need to develop the expertise to appropriately evaluate the exceptions and anomalies observed in the analysis. These and other obstacles are best addressed through a well thought out plan that commits sufficient resources and time.

A decision to invest in implementing or improving data analytic capabilities needs to be appropriately managed to ensure maximum benefit is obtained, with the least amount of cost. A few recommendations to help accomplish these goals are:

1. Align your overall data analysis strategy with your:
   a. Risk assessment process.
   b. Current audit plans.
   c. Long-term audit goals and objectives.

2. Manage your data analysis initiative like a program, focusing on your desired end-state of maturity.
3. Develop a uniform set of analytic practices and procedures across assessment functions.
4. Assign responsibility for data management, quality assurance, and other key roles.
5. Document and/or comment scripted analytics to record the intent and context of the analysis being automated.
6. Review and test analytics being used to ensure the results being generated are accurate and appropriate for the audit step being run.
7. Establish a peer review or supervisory review process of analytics performed to safeguard against the reliance on results generated from using incorrect logic or formulas during analysis.
8. Standardize procedures and tests in a central and secure repository.
9. Safeguard source data from modification/corruption — either through the type of technology being used to conduct the analysis or by analyzing back-up data or mirrored data for audit purposes.
10. Address the potential impact of the analysis on production systems, either by scheduling analysis at off-peak times or by using back-up or mirrored data.
11. Educate staff on how to interpret the results of the analysis performed.
12. Treat training as a continuous process, measured by ongoing growth and continuous development of capabilities.
13. Aim for constant improvement through leveraged use of data analysis software as analytics evolve over time.

7.   Conclusion

Because almost every activity conducted in an organization is either enabled or impacted by technology in one form or another, it is nearly impossible to conduct an audit without using technology. Current audit standards require the use of data analysis for good reason. The data that is processed and collected by organizations is, in essence, the electronic life-blood of that organization. Being able to scrutinize and evaluate the overall health of an organization by analyzing data is a necessity.

To that end, data analysis should be viewed as an enabling technology that can deliver great value to internal audit in the areas of improving efficiency, effectiveness, and levels of assurance that can be provided. Its impact is not limited solely to reducing the amount of time to conduct an audit but also to aid in the detection of errors, control breaches, inefficiencies, or indicators of fraud. Additionally, leading practitioners also are finding better and more effective ways to determine what audits to perform, what areas are high risk, and what business processes require greater attention during detailed audit work. When employed across the audit cycle — from data-driven to insights in risk assessment, planning and preparation, testing, review, and reporting — internal audit can dramatically increase the value it provides and enhance its reputation within its organization.

Deciding where and when to use data analysis should be a strategic decision made by the CAE. By employing data analysis, it must be recognized that there will be changes to what audit staff need to know, what processes and activities need to be carried out, and what technology or technologies can be leveraged to gain the desired benefits. Getting the right data, understanding what the analytics are indicating, and following up on the results of analysis can be a significant task. The returns, however, can raise the level of respect for internal audit departments and the profession as a whole.

Appendix A: Example – Data Analysis for Procurement

Procurement		
Area	**Control**	**Data Analysis**
Purchasing of goods	Application will not allow a duplicate payment to be processed.	Obtain purchase order data Validate that no duplicate payments (same vendor/same account) were processed.
	Purchase orders (POs) older than three months will not be processed.	Obtain a list of all POs processed Determine if POs older than three months were processed.
	The person who creates the PO can't release/approve the same PO.	Obtain a list of all POs created (by originator) Obtain a list of all POs released or approved Determine if any inappropriate segregation of duties (SOD) existed.
Receiving of goods	All goods received (GR) are validated against PO.	Obtain a list of all GR and all POs placed Validate that quantities are the same.
	The person who created the PO can't process any goods that are received.	Obtain a list of who signed for the GR (processor) Obtain a list of who created the PO Determine if any inappropriate SODs existed.
Invoicing	PO should be created before supplier invoice is received.	Compare PO dates against invoice dates and make sure there are no POs dated after invoices dates.
	Amount on PO should agree with amount on invoice.	Compare the PO amount against the invoice amount Validate that there are no differences.
	Segregation of duties (SOD).	Obtain a list of who has processed invoices and who created the PO Determine if any inappropriate SODs existed.
Payment	Application should not allow duplicate payments.	Obtain a list of all payments that have been made to vendors in the last 12 months Determine if duplicate payments have been made, for example: • Same vendor ID and amount but different invoice number. • Same vendor ID and invoice number but different amounts. • Different vendor ID with same bank account detail.
	Segregation of duties (SOD).	Obtain a list of who has processed payment and of who created the PO Determine if any inappropriate SODs existed.
Updating vendor records and adding new vendor files	Ensure that duties are properly segregated to guarantee appropriate control.	Obtain the procurement end-user list (users that have access to the procurement application and the functions that each user has) Determine what functions are conflicting and create a report that identifies those users.

Procurement		
Area	**Control**	**Data Analysis**
	Audit trail that documents what detail was changed when and by what user.	Obtain the audit trails that contain the details of changes that were made to vendor records Determine if only authorized people made changes Identify possible trends of those who are making changes the most.
	Identify key fields (e.g. bank account detail that should be monitored through management sign-off).	Obtain a list of staff bank accounts with direct deposit Compare account information with the bank detail that was updated on the vendor record.
Sufficient application controls to ensure accurate input, processing, and output	1. Valid code test. 2. Check digit. 3. Field check. 4. Limit test. 5. Reasonableness check. 6. Sequence check. 7. Batch control totals.	1. Obtain a monthly download of program code within the procurement application → Determine if any changes were made to the code through data analysis. 2. Obtain the standing data of vendors → Validate that the Income Tax number captured is the correct length. 3. Obtain the standing data of vendors → Validate that only numerical values are captured in the bank account and phone number fields. 4. Obtain a list of all procurements that were made in a month → Validate that all payments above a certain amount (e.g., US $50,000) were authorized by the appropriate user. 5. Obtain a list of all procurements made in a month → Create a trend analysis, per vendor or per procurement type, to identify transactions out of the ordinary.
Value adding services to organizational users	N/A	1. Total dollars spent. 2. Average transaction amount. 3. Transactions per vendor. 4. Dollars spent per vendor. 5. Sort transactions by vendor or commodity. 6. Trend analysis (e.g., seasonal products). 7. Budget vs. actual 8. Age analysis (e.g. GR vs. invoice date)

Appendix B: Ranking Matrix for Data Analysis Software Selection

Need: 0=Needless; 1=Nice to Have; 2=Desirable; 4=Mandatory.		Need
Internal Auditing Strategic Objectives		
1	Software is easy to learn and use	
2	Competitive advantage	
3	Minimize reliance on IT professionals	
4	Improve work accountability, responsibility, and supervision	
5	Enforces production program change controls	
6	Reliability: bug free, speed, work like a professional	
7	Portability: runs on a laptop	
8	Scalable: grow from desktop to server without learning new software	
9	Data integrity and security: client data is protected from auditor change	
10	Collaborative features	
11	Supports development of automated and continuous programs	
12	Compatible with electronic workpapers	
13	Improves documentation of audit work completed	
Provider & Implementer Support		
14	Global presence	
15	Years in business	
16	Multiple languages	
17	Help desk available	
18	Ease of doing business; knowledgeable in auditing needs	
19	Regular software upgrades	
20	Training readily available	
21	User group program for networking with other users of the software	
22	Knowledgeable consultants independent of the provider readily available	
23	Getting started programs available	
Technical Features & Functionality		
24	Import all file types used by the organization	
25	Handle large file record sizes	
26	Handle large data volumes	
27	Ease in validating and reconciling data import	
28	Modify imported data field properties	
29	Support search for text, numbers, time	

GTAG — Appendix B: Ranking Matrix for Data Analysis Software Selection

Need: 0=Needless; 1=Nice to Have; 2=Desirable; 4=Mandatory.		Need
30	Project visual chart or mapping of data actions performed	
31	File join/merge/compare	
32	File append	
33	Visual connector	
34	Sorts, indexing, filtering, and fuzzy logic	
35	Summarization	
36	Extraction	
37	Pivot table	
38	Stratification	
39	Gap detection	
40	Aging	
41	Compare data to predicted data according to Benford's Law	
42	Advanced statistical analysis: correlation, trend analysis, time series	
43	Sampling	
44	Statistical analysis	
45	Export to typical office applications	
46	Create custom reports and graphics	
47	Create simple and complex calculated fields	
48	Data cleansing tools − @functions available	
Cost		
49	Software purchase	
50	Job aids − automated scripts and specialty components	
51	Upgrade fees	
52	Annual help desk support	

Appendix C : Audit Department Data Analysis Usage Maturity Levels

The following table can be used by audit leaders to assess the maturity level of their data analysis usage within their departments, with an eye toward increasing the levels of assurance and value-adding services they can provide. Alternatively, the descriptions and attributes listed therein also can be used to formulate a data analysis strategy that will improve efficiency and effectiveness within their departments. It is recognized that different maturity levels can exist within a single internal audit group, depending on which part of the organization they are auditing.

Level	Description	Attributes
Fully Optimized	Data analysis is engrained in all audit programs. The audit department relies heavily on data analysis technology during all stages of the audit plan. Many audit processes are automated to ensure the quality and consistency of results. Data analysis technology is acknowledged as an essential component in enabling the audit function to complete their audit plans.	Companywide recognition and support for data analysis as a core competency of the internal audit function to support the expected assurance and consulting services.
Integrated	Data analysis is used in every applicable audit engagement, and in each stage of the audit cycle from risk assessment, planning, preparation, testing, issue follow-up, and reporting. Proficiency in data analysis technology is a job requirement for some or all of the audit staff, depending on its size and make-up. Close integration exists with IT and the rest of the organization regarding access to pertinent data and dissemination of results.	Top-down support to meet functional strategic directives is in place. It is recognized that data analysis can assist internal audit in providing heightened levels of assurance by looking for unauthorized, incomplete, or inaccurate data or seeking indicators in the data that can lead to recommendations to improve the organization's overall performance.
Isolated and Occasional	The audit department has some individual or single resources versed in the use of data analysis software. Oftentimes the role of data analysis has been centralized to one individual. Application of data analysis in audit programs is sporadic and unformulated. Challenges exist in acquiring data from IT.	Some false starts and activities not necessarily sustainable for a long period. Acquire professional data analysis tools without the opportunity to fully implement. Realize that "peer" groups may be making significant strides. Push for data analysis skills more bottom-up driven.
Reliant Primarily on Spreadsheets	Audit processes make use of spreadsheets for light analysis (sorting, calculating, control totals, sums, etc.), sampling of small data sets, limited use of macros to locate anomalies in subpopulations of data.	Starting to recognize the need for independent verification and objectivity. Starting to become aware of the possibilities. Generalized software tools employed with known limitations.
Print/ Paper-based	Auditors spot-check printed copies of documentation seeking evidence of controls compliance.	Relying on the work of others. Development of data analysis skills are in its infancy, in the planning stages at best.

Authors and Reviewers

Authors:

Altus J. Lambrechts, CISA, CRISC
Jacques E. Lourens, CIA, CISA, CGEIT, CRISC
Peter B. Millar
Donald E. Sparks, CIA, CISA

Reviewers:

The IIA thanks the following organizations that provided valuable comments and added great value to this guide:

The IIA–South Africa
Chartered Institute of Internal Auditors (U.K.)

GTAG®

About the Institute

Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs, Fla., USA. The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator.

About Practice Guides

Practice Guides provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. Practice Guides are part of The IIA's IPPF. As part of the Strongly Recommended category of guidance, compliance is not mandatory, but it is strongly recommended, and the guidance is endorsed by The IIA through formal review and approval processes.

A Global Technology Audit Guide (GTAG) is a type of Practice Guide that is written in straightforward business language to address a timely issue related to information technology management, control, or security.

For other authoritative guidance materials provided by The IIA, please visit our website at www.theiia.org/guidance.

Disclaimer

The IIA publishes this document for informational and educational purposes. This guidance 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 guidance.

Copyright

The Institute of Internal Auditors

www.theiia.org