



WHITE PAPER

Best Practices for the Use of Data Analysis in Audit

John Verver, CA, CISA, CMC

CONTENTS

- Executive Summary 1
- The Evolving Role of Audit Analytics 3
 - Applications of Audit Analytics 3
 - Approaches to Audit Analytics 4
 - Value of Data Analysis in Audit Today 4
- Best Practices for Audit Analytics 5
 - 1. Data Access & Management 5
 - 2. Quality & Control of Audit Analytics Processes 8
 - 3. Collaboration, Efficiency & Sustainability 9
- Seven Practical Steps to Establishing Best Practices for Audit Analytics 12
 - i) Understand Your Requirements 12
 - ii) Understand Your Technology Environment 12
 - iii) Develop a Data Analytics Strategy 12
 - iv) Define Your Audit Analytics Architecture 13
 - v) Plan Your Technology Rollout 13
 - vi) Assign Roles and Responsibilities within Your Audit Team 13
 - vii) Implement a Training Program 14

EXECUTIVE SUMMARY

Over the past 20 years, data analysis has become an essential part of the audit process for the vast majority of audit organizations. Using data analysis in audit (generally referred to as “audit analytics”) has already provided significant benefits for audit organizations of all sizes across a broad range of industries, but there is still much progress that can be made by optimizing the audit analytics process.

Audit analytics include a wide range of types of application, varying by size and sophistication of the audit organization, as well as by industry. Applications range from ad hoc analysis to support a given audit objective, through to repeatable automated procedures and on to continuous auditing and monitoring. There are common best practices that apply no matter where an organization operates on the continuum of audit analytics, nor how far they have progressed from a traditional cyclical approach to a continuous and risk-based model.

In order to apply best practices and achieve the highest value from audit analytics, three key areas must be addressed:

■ Data Access and Management

Effective data access and management requires seamless security, understanding of organizational practices, and of course, access to large volumes of data. While these are significant challenges for many audit organizations, creating and maintaining an audit data repository is perhaps the most common and effective solution. This repository consists of sub-sets of enterprise data, representing only the data that is needed for audit purposes. The repository runs in a secure server environment that is subject to enterprise standards for data security and management. Developing and maintaining an “intelligent” data dictionary within the central server environment is another key strategy that auditors can use to better describe data elements by purpose and significance.

Maintaining the audit repository in a secure server environment is a critical way to ensure data integrity, effective management, and to quickly process large data volumes for both interactive inquiries and automated tests. Server data security is typically far more effective than controls implemented on individual laptops or PCs, which is why server environments are strongly recommended with audit analytics.

■ Quality and Control of Audit Analytics Processes

The most effective quality assurance solutions are twofold: developing standard procedures and tests and creating audit analysis process controls. In a central server environment, audit organizations can house procedures and test libraries for audit analytics, while providing core access to logs and documentation.

Maintaining control over the audit analytics process is also best achieved in a centralized location. This is an effective way to track and reconcile totals from one testing process to another to ensure that procedures are performed on a full and correct data population. A specialist can also review procedural logic and tests can be “locked” to prevent any accidental or deliberate procedural changes.

■ Collaboration, Efficiency and Sustainability

Audit analytics are most effective when the analysis is a fundamental part of the audit strategy, and used in an environment of collaboration, shared knowledge, and repeatable processes. It’s critical that technically proficient specialists are not solely responsible for creating and maintaining test procedures. Instead, practices should be captured and sustained in a centralized server system

that can be independently accessed (without IT intervention) and repeated by auditors with a range of technological skill.

A centralized approach also ensures that complex data processing can be achieved with maximum efficiency and minimal downtime. While laptops and individual PCs have made remarkable gains in speed and power, they cannot match the security and processing ability of a server system. Additionally, analytic procedures can be closely linked with audit programs and working papers – enabling auditors to move smoothly between an audit analytics process and specific audit programs and working papers.

Imperative to the successful use of audit analytics and audit best practices is training on the effective use of technology, as well as education on continually evolving audit processes. Best practices in audit analytics are most effectively delivered through a managed, centralized technology that provides optimized and secure data access, quality control, knowledge sharing, and automation of audit tests for long-term sustainability.

THE EVOLVING ROLE OF AUDIT ANALYTICS

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 organizations now aim to integrate audit analytics throughout the audit process and expect all auditors to have an appropriate level of technological competency.

Although a wide range of data analysis technologies can be applied to audit, there has also been widespread acceptance within the audit professions that data analysis technologies designed specifically for audit application have distinct advantages over more generic technologies.

Applications of Audit Analytics

Here are several areas in which audit analytics have been applied successfully:

Analytical Review

Typically, this involves a preliminary analysis of all transactions that take place within a given business process during a set period. This results not only in additional insight into the nature of the business activities, but can also identify trends and anomalies that may indicate potential risk areas and concerns that require specific audit focus.

Controls Assessment and Testing

This usually involves two primary approaches:

- Examination of 100% of transactions to determine whether each transaction appears to comply with a specific control rule
- Examination of 100% of transactions to determine whether there is an indication of activities occurring for which no control has been implemented

Substantive Testing

Analysis of transactions (or a statistical sample) to determine whether they are complete, valid and accurate.

Fraud Detection

Analysis of transactions to identify fraud indicators.

General Analysis and Reporting

The general application of audit analytics to identify anomalies in business processes or transactions, resulting in audit reports highlighting anomalies and providing management with recommendations to address shortcomings.

Financial and Non-financial Transactions

Audit analytics are most frequently applied to transactions in financial or operational audits. However, they have also been proven to be very effective in IT audit and security reviews, where, for example, they are used for analysis of Segregation of Duties, of system configuration settings and of systems access logs.

Approaches to Audit Analytics

Data analysis is used within the audit function in two primary ways:

Manual Approach

Interactive use involving **ad hoc** procedures that are typically explorative and investigative in nature in order to support inquiry, testing and analysis in support of a specific audit objective.

Automated Approach

An automated approach includes a series of steps that can be easily repeated when needed. The automated approach can be delivered either through repetitive analysis or in a continuous mode or, optimally, a combination of both:

Repetitive

- the periodic running of automated **standard audit tests** to improve the efficiency, consistency and quality of audits

Continuous

- the continued execution of **automated audit tests** to identify errors, anomalies, patterns and exceptions as they occur
- **continuous monitoring** in which all transactions within key business processes are automatically tested for compliance using controls on an ongoing basis and anomalies are identified in a timely manner for management response

Value of Data Analysis in Audit Today

The benefits of performing audit analytics fall into several main categories:

Productivity and Cost Savings

Audit organizations refer to dramatic reductions in time requirements for audit procedures when using data analytics. This productivity improvement typically translates into the ability to deliver considerably more with current staff levels or the ability to reduce audit staff requirements.

In many cases, the effective use of audit analytics reduces the need for travel and its associated costs, as many audit procedures can be performed at a central location. Travel to other sites is then limited to locations when audit analytics procedures indicate that it is warranted, as a result, for example, of identifying apparent control problems.

Quality

Audit analytics generally allow far more extensive audit procedures to be performed, particularly substantive audit testing. Instead of performing judgmental or statistical sampling, testing can be conducted across 100% of transactions in a given audit area.

To ensure quality in audit analytics, it is important to maintain detailed audit logs of all analytics procedures performed. The technology deployed should have the ability to log each step of the analysis, representing a comprehensive audit trail. This enables organizations to automatically document procedures as they take place – translating into both reduced time requirements and higher quality audit documentation.

Independence

In cases where audit analytics technology is not employed, many audit departments depend on an organization's Information Technology function to provide data access, perform analyses and produce reports. This adds an extra step that can slow down the delivery time between extract and analysis, and also erodes the independence of the analytic procedures themselves. If an auditor needs to describe the nature of analysis and reports to an IT programmer, this immediately reduces the auditor's independence.

Given capabilities for independent data access and analysis, an auditor becomes more efficient and more independent. The ability to perform independent analysis is at the core of the concept of "the truth is in the transactions." By independently examining an entire population of transactional data, an auditor can more effectively determine the truth of what has occurred within a given business process and measure the effectiveness of controls.

Audit Risk

The use of audit analytics can significantly reduce audit risk. Traditional audit approaches relied upon judgmental or statistical sampling for both substantive and compliance testing. However, the use of audit analysis software allows entire populations to be subjected to broad ranges of test procedures. By comprehensive testing of 100% of transactions, auditors are able to achieve increased confidence and reduced risk in their audit procedures.

Supporting Internal Audit's Changing Role

The role of internal audit is evolving in many organizations. There is a move away from the traditional cyclical approach to audit to one in which audit continually assesses areas of greatest risk and performs in-depth audits in specific areas as required. Continuous auditing and monitoring techniques can enable this changing role by providing ongoing automated analysis that highlights areas of greatest risk and audit concern. Instead of providing a cyclical audit report to management, the results of continuous auditing and monitoring procedures can also be immediately provided to management to identify areas requiring investigation and response.

BEST PRACTICES FOR AUDIT ANALYTICS

Data analysis has added tremendous value to the audit process and to audit organizations. However, many opportunities remain for wider and more effective use of audit analytics.

The remainder of this paper identifies the most common issues that must be addressed to maximize the value of audit analytics and outlines practical steps for establishing best practices.

Audit analytics best practices can be grouped into three categories:

1. Data Access & Management

Challenges:

- Data access
- Understanding data
- Data Security
- Managing large volumes of data

Data Access

In order to perform audit analytics procedures, auditors need effective access to the data that underlies a specific business process area. This includes transactional data as well as, in many cases, master file and system configuration data. Although Information Technology departments can usually be convinced to give data access rights to auditors, there is often reluctance to provide direct access to live operational system data and concern that creating entire ERP database copies will be impractical and inefficient. As a result, auditors can spend considerable time negotiating with IT to get working access to the data they need to analyze.

Understanding Data

Once an auditor has access to the appropriate datasets and databases, the auditor must understand what specific data elements are needed to support a particular analysis. When faced with potentially tens of thousands of data tables in an ERP, each of which may contain a large number of cryptically named data fields, this can be a considerable challenge.

Data Security

Maintaining effective data security is increasingly recognized as a critical risk area for organizations. The loss of control over data security can have severe ramifications for an organization, including regulatory penalties, loss of reputation and damage to business operations and profitability.

Organizations, specifically IT departments, often create extensive policies and procedures to maintain security and control over data. However, it has been common practice for some audit organizations to extract critical data and download it to audit workstations or laptops for analysis. Although this can be an effective way to provide auditors with direct data access, it means that audit may well be circumventing established data security measures. Even if some form of encryption is used, the loss of control over one audit laptop containing critical data can create a major exposure for an organization.

Managing Large Volumes of Data

The use of audit analytics often involves processing very large volumes of data, involving many millions of transactions. Managing such data in an efficient way can be a challenge, particularly when analytics involve the creation of multiple sub-sets of data and index files. Maintaining data in a way that supports the most efficient processing speeds can also be a challenge and result in delays while auditors wait for processing to complete on their laptop or workstation. Many auditors are not familiar with the appropriate techniques for optimum data management and processing. In the case of analytics performed on local area networks, processing large data files will often result in performance degradation over the entire Local Area Network (LAN).

Solutions:

- Establish an audit data repository
- Develop an "Intelligent" data dictionary
- Utilize a server environment for data management, control, security

Establish an Audit Data Repository

Creating and maintaining an audit data repository, which runs within a secure server environment that is subject to enterprise standards for data security, is the most common and effective overall solution for the issues outlined above.

The value of establishing a secure audit data repository is becoming increasingly well documented. The repository consists of sub-sets of enterprise data, representing only the data that is needed for audit purposes. This means that the data volumes are large, but dramatically smaller than those contained in

enterprise ERPs and application systems. Data may also include external data, such as industry statistics that can be used for benchmarking comparisons and analysis.

The data can physically reside on the audit data repository server, or it may be a virtual part of the data repository with the data residing on enterprise systems, with links to the repository by the audit server software that manages the audit data dictionary. Where data is physically downloaded, it is physically refreshed on a regular basis to ensure the data is as current as possible for audit analytics purposes.

Maintaining a sub-set of enterprise data on a dedicated server also means that there is no impact on the performance of operational systems when the auditor performs extensive analysis.

Develop an "Intelligent" Data Dictionary

Since the audit repository only contains data needed for typical audit purposes, all of the data elements can be described in a way that make sense to the average auditor. For example, instead of referring to CWID (PA0901_UNAME) and field PA0901_SORTL in table /BAY2/UBEMWFGRAD, the data can be described more helpfully as "P.O. approver's authorization limit."

The data dictionary should also be structured according to the typical audit area, and key data elements described in terms of the significance of the data for a specific audit test. Developing and maintaining the audit data dictionary for all auditors' use is a centralized function that is best managed on a central audit server environment.

Utilize a Server Environment for Data Management, Control and Security

Analysis of a complete data population of the general ledger of sub ledger balance is critically important for a successful audit analytics program. In practice, this need is often overlooked, meaning that analytic procedures result in incomplete or invalid conclusions. By establishing and managing an audit data repository, the reconciliation process can be performed centrally and repository users can rely on the completeness of the data population.

Ensuring that run-to-run control totals and processing logs are maintained and available for review is another key aspect of data control. This means that as a series of analytical procedures are performed – some on sub-sets of the transactions representing the entire audit area – auditors can determine that all relevant data has been included in a specific test and that no transactions were accidentally omitted or inappropriate transactions included.

Although it may be possible to follow some of these procedures in an environment where an auditor works with data on a laptop or desktop computer, it is considerably more effective and efficient to centralize these control procedures in a standardized server-based environment.

Server environments are designed to efficiently support and enforce enterprise standards for data access and security. Although security standards and procedures can be established for end-user computers, such as laptops, desktops and Local Area Networks, they are typically easier to circumvent and harder to enforce. Circumvention of control standards may be done with the best of intentions, for greater efficiency or ease-of-use, for example. However, it can still result in compromised data security if a laptop is lost or a guest uses an insecure desktop machine when the owner is away.

Although an audit department's IT auditor may be responsible for auditing data security throughout the enterprise, it is not unheard of for an audit department itself to fail to comply with enterprise security standards in its interactions with critical data.

The security of server data access is usually far more effective than that of end-user computers, both at the operating and database systems levels, and particularly if servers are subject to central security

management. For this reason, server environments are particularly recommended for best practices in audit analytic use.

The most effective way to maintain an efficient centralized audit data repository is to appoint an individual who is responsible for data management and standards. Frequently this includes responsibility for data update processes, data dictionary maintenance and standards for analyzing and managing audit data.

Effectively using audit analytics requires that large volumes of data be processed very rapidly. This is necessary for both interactive inquiry processes and automated tests, including continuous auditing and monitoring. Although laptops and desktops are increasingly powerful, both in terms of processors and data storage, servers are designed for heavy duty processing of very large data volumes and support multiple users with minimal impact on end-user response times. Servers have become the standard for most audit organizations that deal with large data volumes and a wide range of analysis tasks.

2. Quality & Control of Audit Analytics Processes

Challenges:

- Effective control of audit analytics processes
- External audit's reliance on work performed by internal audit

Effective Control of Audit Analytics Processes

Although many audit organizations encourage the use of audit analytics, it is not uncommon for both specialists and generalists to be given a relatively free hand in the procedures they perform. This opens up opportunities for a flawed approach, which leads to incorrect or inconsistent conclusions. For example, if the underlying business process is not fully understood, the data fields used for analysis may not be valid for a given audit objective, or the data manipulation logic for the analysis may itself be wrong.

In the case of standard audit analytics, unless the tests are appropriately secured, users may make changes that invalidate the test. It may even be undesirable to allow all auditors access to procedural details in the cases of more sensitive analyses.

External Audit's Reliance on Work Performed by Internal Audit

Many internal audit departments perform procedures that support the external audit process. The extent to which external auditors can rely on the work of internal auditors varies, but there is often increasing expectation that external audit firms will reduce their work by relying on internal audit's procedures. When audit analytics are performed in an ad hoc and uncontrolled way, it is often more efficient for an external auditor to repeat the process rather than spend considerable time determining whether the procedures and results can be trusted.

Solutions:

- Implementation of a central server environment
- Institute audit analytics process control procedures

Implementation of a Central Server Environment

Developing and managing a central library of standard procedures and tests is key to ensuring that audit analytics are performed at the highest level and conducted in a controlled manner. The standard procedures can include direction on the type of steps that must be performed for all audit analytics as well as the type of analysis required to achieve a given audit objective.

Although specialized audit analytics software such as *ACL* automatically logs procedures performed, best practices also involve standards on the use of procedural documentation and comments that are produced by auditors and included in the audit logs.

Best practices typically require a central server environment to house the details of procedures and test libraries, while providing central access to documentation and logs for management and review purposes.

Institute Audit Analytics Process Control Procedures

Control over the integrity of the audit analytics process is critical and often overlooked. Maintaining effective control involves, for example, procedures to ensure that totals are maintained both of transactions processed and of key numeric fields. Although audit technology such as *ACL* does this automatically, it is important to track and reconcile the totals from one process to another to ensure that audit procedures are performed on the entire correct population or sub-set of population of data.

The logic of analytics procedures also needs to be reviewed and confirmed by a specialist to ensure that the analysis is accurate and truly supports a specific audit objective. This is usually easy to achieve with standard tests. Ad hoc procedures, however, require more care to ensure that the procedures and conclusions are correct.

Although standard analytics help to ensure test validity, care must also be taken that inappropriate changes are not made to the logic, either accidentally or deliberately, by users. Using “locked” tests can prevent such changes. In cases where the audit procedures are very sensitive, access can be limited to selected audit staff or the analysis code for critical test steps can be encrypted so that full security is maintained.

A central audit server environment is key to effectively controlling, reviewing and managing a comprehensive range of staff audit analytics procedures. It also gives external auditors the ability to review procedures in an efficient way and to determine the reliability of those procedures. External auditors can then place more trust in well controlled, centrally managed procedures and manage their work accordingly.

3. Collaboration, Efficiency & Sustainability

Challenges:

- Sustainable knowledge sharing and retention
- Selecting the right technology
- Integration with other applications

Sustainable Knowledge Sharing and Retention

Although the value of audit analytics is generally well recognized, for many organizations, extending use to a far wider group of auditors would reap additional benefits. In order to achieve more widespread use, knowledge sharing and effective collaboration are critical. If knowledge is isolated among individual auditors and information is difficult to share and lever, the overall benefit can be considerably reduced.

It is common for audit organizations to rely on a small number of specialized technical auditors for much of the work involving audit analytics. Specialists can spend considerable time developing sophisticated and comprehensive test suites and automated audit systems, which provide much value. However, depending on specialists can be risky. If a specialist leaves the organization, it can rapidly become very difficult to maintain or enhance the system – and in some cases, to use it at all.

Selecting the Right Technology

Laptops and individual PCs are lacking in security and processing power. The challenge is finding the right combination of data access and processing power capabilities.

Integration With Other Applications

It is also becoming increasingly important to connect or integrate audit analytics procedures in an efficient way with other software technologies, such as audit working papers and risk and compliance management software.

Solutions:

- Create and foster a collaborative sharing environment
- Leverage technology for efficiency gains
- Implement technologies that integrate

It is critical to make audit analytics a fundamental component of an audit strategy and to establish a centralized system approach that focuses on collaboration, knowledge sharing and efficient, repeatable processes. Specialists' skills and experience should be harnessed in a sustainable way to maximize their value and avoid dependency.

Create and Foster a Collaborative Sharing Environment

Sharing of knowledge and information typically falls into the following areas: Projects, Data, Data definitions/dictionaries, Standard test libraries, and Results

All of the above are best housed in a centralized, secure server-based environment designed to efficiently manage and share a wide variety of data and information, so that organizations can avoid the risks and inefficiencies that arise when individual audit analytics users maintain systems independent of each other.

The best practice model combines the role of technology specialists with the functions of financial and operational auditors. The key is to maximize specialists' value and to harness their knowledge and work in a way that minimizes specialist dependency. Specialists have a key role to play in working with the IT department to establish data access and data update procedures, as well as defining the audit data dictionary. They are often critical to developing standard audit tests and reviewing analytical logic.

Clearly, the goal is a sustainable approach in which the specialists' knowledge is captured within a centralized audit analytics server system and made available on an ongoing basis to the benefit of more generalist financial or operational auditors.

Collaboration is important on a number of levels. Collaboration within internal audit means that all auditors can share and benefit from the audit analytics work of others. In particular, it means that managers and specialists can easily review the work of others through one central secure and controlled system.

Collaboration between internal and external audit is important in order to maximize the reliance that external audit can place on the work of internal audit. Again, a central audit analytics server system can allow external auditors to access procedures performed in an efficient manner and conclude on the procedural integrity.

A successful overall audit analytics process also involves collaboration with an organization's Information Technology department. A well-managed centralized audit data repository with standard processes for accessing and updating data can substantially reduce the ongoing effort required by IT.

Maintaining data within a secure system that is subject to the same security and data administration standards as other critical enterprise data can provide assurance to an IT department or a CIO if there are concerns about data moving outside of the secure environment.

Leverage Technology for Efficiency Gains

Specialized audit analytics software such as *ACL* can be remarkably powerful and fast when processing large data volumes. However, analytics can also be applied in very inefficient ways, sometimes without the user realizing, which leads to wasted time and processing resources.

A centralized approach enables reviews to be performed more easily and standard procedures to be applied, ensuring that analytics processes are optimized to best address complex procedures and very large data volumes in an automated and easily repeatable way.

Though laptop and desktop computers are very powerful, server technologies are designed to process large data volumes with the highest degree of efficiency. The use, for example, of multiple processors in servers and system software that manages resource allocation can maximize overall performance while avoiding negative impact on performance for other users. Combined with the server's ability to directly access and process data from operational systems, often without needing to download the data, can further enhance overall performance times. Where necessary, analysis can be scheduled to run automatically in off-peak hours, further reducing the impact on systems' performance.

Using servers for heavy duty processing also avoids the inefficiencies of tying up end user workstations/laptops for long periods of time. Developing centralized procedures for clear documentation and self-documentation can boost the overall efficiency and effectiveness of audit analytics.

Implement Technologies That Integrate

It is preferable for audit analytics procedures, whether ad hoc, standard tests or part of continuous auditing and monitoring processes, to be closely integrated with audit programs and working papers. An auditor should be able to move directly from a specific audit program step and working papers to an audit analytics process. The results of the analysis are then linked directly back to the working papers. As most audit working paper software is server based, integration with audit analytics becomes easier, in both technical and procedural terms, when audit analytics software is also based around the use of server systems.

The same benefit applies when an additional technology component is involved, such as controls and compliance management software. A three-way level of integration may be desirable if, for example, an audit procedure refers to a specific control identified in a compliance management system, as well as to the results of control testing and transaction monitoring performed within a business process area.

SEVEN PRACTICAL STEPS TO ESTABLISHING BEST PRACTICES FOR AUDIT ANALYTICS

In establishing an effective audit analytics environment within which to execute best practices, a number of practical steps need to be followed. All too often these steps are overlooked leading to lengthy delays, mismatched expectations and deferred return on the investment in technology.

The decision to implement an efficient and effective audit analytics solution is a strategic one and not a matter for a tactical approach. The strategic approach requires audit management to engage others in the organization to explain desired outcomes, manage changes to existing procedures and protocols, and to plan the transition to a more centralized, managed and secure approach to audit analytics.

i) Understand Your Requirements

Identify what parts of the organization you are going to audit and which business processes can be scrutinized using data analysis. Defining your objectives up front will save considerable time over the long run and help you in planning what data sources you will need, who you will have to work with to gain access to the data, and whether or not this is a task that you will want to automate as part of a continuous auditing system.

Part of defining and understanding your requirements includes where analytics are going to be used. Audit analytics can be used throughout the audit cycle. Consider audit analytics use in Planning, Preparation, Testing, Review and Reporting.

Use audit analytics in the audit planning stages such that high-risk areas or indicators of non-standard operations can be identified. Identify where automation of tasks can be leveraged in data access and preparation. Plan and lay out what analytics you want to run and how often they should be run given the level of risk to the organization. Determine up front what sorts of reports you are going to want to generate and who will receive those reports – recognizing that different users consume information in different formats and levels of detail.

ii) Understand Your Technology Environment

Engage IT early in the process and work with them to identify and characterize the diverse operating systems, applications and data sources you will need access to. By collaborating with IT early, you will be able to establish a technical architecture that will suit your analytical requirements and support the audit efficiencies you are seeking. By engaging IT early, and explaining to them your overall objectives and reasons for acquiring data, you will find them a very useful and helpful resource.

iii) Develop a Data Analytics Strategy

Your data analytics strategy is a natural extension of your overall requirements. The strategy needs to include the elements of data accessibility, data analysis protocols, establishment of business process and internal control standards and the overall review of analytics performed.

Data Accessibility: IT is charged with safeguarding the data of the organization, and audit needs access to that data to fulfill its mandate. It is necessary to work with IT to set up server profiles and database profiles for the audit team to gain secure and authorized access to the data and the hardware platform(s) where the processing will take place.

Data Analysis Protocols: Avoid data duplication wherever possible. It creates data storage challenges and is often unnecessary. With the right technology, you can read data directly from databases. When

data extraction is required for point-in-time analysis, extract data to the central audit analytics server where appropriate. Avoid downloading data to the client PC – it isn't necessary and introduces other challenges such as maintaining the security and confidentiality of source data and analytical results.

Process and internal control standards: Part of your audit analytics strategy needs to include your understanding of business processes and associated internal controls. By flow-charting business processes, you will be able to identify what data sources need to be accessed, analyzed and compared in order to validate the integrity of the process. Once this is understood, you will be able to identify areas where internal control breakdowns are likely to occur – such as where processes span different applications or systems. Audit analytics can be used to bridge gaps in automated processes so that internal control standards can be maintained.

iv) Define Your Audit Analytics Architecture

Once you understand your environment, work with IT to design your audit analytics architecture. Where will you set up your centralized and secure audit environment? What sort of hardware will you need given your data access and storage requirements? While defining your architecture, include a documentation phase where you can define the contents and scope of your audit data repository and data dictionary. The data repository requirements and data dictionary definitions will change over time as the organization's IT environment changes and your audit requirements adjust to emerging risks.

v) Plan Your Technology Rollout

Establishing a centralized, secure and managed audit analytics environment needs to be a coordinated and planned activity. Not only will hardware and software need to be installed and set up, but authorized access to systems, databases and directories will also need to be established. People will need to be trained on the system and processes documented.

It is highly recommended to identify and plan for these elements to ensure a smooth and efficient implementation. Without a technology rollout plan, lengthy delays are almost a given. Deploying a best practices audit analytics environment involves people from a number of different functions – from audit to IT to management. Coordination of these busy resources ensures that your access to systems and databases coincides with the installation of hardware and software and with the understanding of how internal controls are going to be tested.

vi) Assign Roles and Responsibilities within Your Audit Team

Audit is a team sport and like all teams, people need to play different positions. The key to highly effective and winning teams is to place people in roles to which they are best suited.

Certain tasks are technical in nature and others less so. In establishing a centralized audit analytics solution, you should leverage the technical expertise on your team by assigning them the key role of liaising with IT on data access issues. By assigning a technical resource in this role, you will be able to free up less technical users from this task and have them concentrate on the other aspects of the system – such as auditing the data, documentation of processes, standards or control tests.

Others should be assigned roles in Security and Administration. This role is key in assuring that access to data and results is consistent with internal security standards and protocols and that no unauthorized access to information is granted. The administrative aspect of this role includes the management of audit standards and the documentation of the centralized data dictionary. This is a very important role in assuring the integrity and continuity of the audit analytics system as people circulate through the audit team over time. This role should also include specific responsibility for implementing policies for data retention and archiving, including not only transaction data but also activities logs and automated routines.

Audit team members who have an aptitude for critical thinking in the use of audit analytics should be assigned the role of test creation, standardization and optimization. By placing an expert in this role, audit management can be assured that the tests being run and the results being generated are of the highest standards and will not be subject to the shortcomings of inconsistent testing.

Audit Management's role is one of oversight and review. Review of tests, results and documentation needs to be accomplished on a routine basis. This will ensure that the overall coverage, consistency and quality of audits are maintained on the team and that the audit function is performing effectively. Review needs to be conducted in all aspects of the audit analytics solution – from planning to data acquisition to testing, reporting and follow-up.

vii) Implement a Training Program

Finally, an effective training program is required to expand the knowledge of the audit team in the use of audit analytics across the audit cycle. It is only through a comprehensive and accredited curriculum of study that audit management can be assured of success in the deployment of audit analytics technology. With effective training, one will be able to gain higher productivity in the use of audit analytics, reduced learning curves when applying analytics to new areas of the business, and a greatly accelerated return on investment of the technology. It will also provide added confidence in analytical results and that audit objectives are being met.



ACL Headquarters

T +1 604 669 4225
F +1 604 669 3557

■ acl.com
info@acl.com

COMPANY OVERVIEW

ACL is the leading global provider of Audit Analytics to financial executives, compliance professionals, and auditors. Combining market-leading data analytics software and professional services expertise, ACL solutions give organizations confidence in the accuracy and integrity of transactions and the effectiveness of internal controls underlying increasingly complex business operations. Since 1987, ACL's proven technology has enabled financial decision-makers to assure controls compliance, reduce risk, detect fraud, enhance profitability, and achieve fast payback.

Our international customer base includes 70 percent of the Fortune 500 companies over two-thirds of the Global 500, the Big Four public accounting firms, and hundreds of national, state, and local governments. ACL software solutions are delivered in multiple languages in more than 130 countries to over 170,000 licensed users through a global network of ACL offices and channel distribution partners.