

# The Mechanics of Data Analysis for Fraud Detection

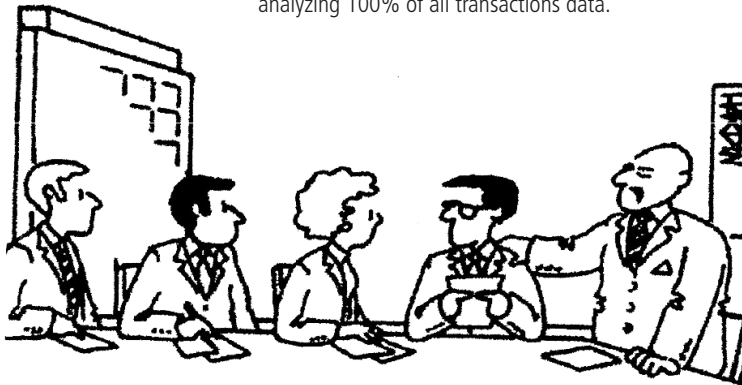
## Part I: Data Access

Auditors, fraud examiners, and compliance professionals are being pressured to shorten audit cycles, increase efficiencies and coverage, and focus resources on investigating and assessing areas of high risk. These pressures, combined with a global economic downturn, are changing the scope of your work and how you need to manage it.

Fraud, error, waste, and abuse are risks that essentially every organization faces. There's always a risk that revenue will be lost; that someone will misappropriate funds, abuse a corporate program, or make mistakes costing the company money and credibility.

The right data analytics program helps organizations stem losses due to fraud error, waste and abuse. The first priority is to identify areas of high risk. Then you need to implement internal controls to mitigate risk in these areas. Finally, it's critical to test these controls by analyzing 100% of all transactions data.

### Consul"toon"



**"Hard figures are not available, but Henry's poem explores the essence of our situation."**

### Easy access to all data

To perform data analysis for fraud detection, you need access to the data that underlies a specific business process area. These include transactional data as well as, in many cases, master file and system configuration data. Gaining access to live operational system data is cited among the top challenges by internal auditors today.

The most common and effective overall solution is the creation and maintenance of an **audit data repository**, running on a secure server environment, that is subject to enterprise standards for data security and management.

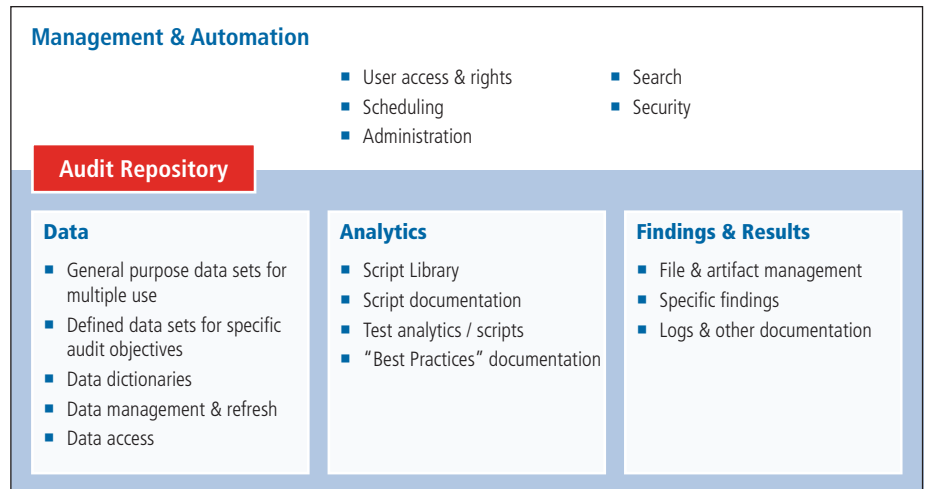
The repository consists of sub-sets of enterprise data, representing only data that is needed for audit purposes. This means data volumes are large, but dramatically smaller than those contained in enterprise ERPs and application systems. In some cases, the repository merely consists of pointers to the actual data source. Where data is physically downloaded, it is automatically refreshed on a regular basis so the data is always current for audit analytic purposes.

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

Since the data in the audit repository only contains data needed for analytics purposes, all the data elements can be described in a way that makes sense to the average auditor or fraud investigator.

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.

Security is tighter and more effective when accessing data through a server, particularly if servers are subject to central security management. Because of this, server environments are particularly recommended as a best practice in data analytics for fraud detection and prevention.



## Data Control & Security

A critical aspect of using data analytics for fraud detection is the need to ensure the data being analyzed is the same complete data population that comprises a general ledger or sub ledger balance. This imperative is often overlooked, meaning the analytic procedures performed will result in incomplete or invalid conclusions.

The other key aspect of data control is to ensure run-to-run control totals and processing logs are maintained and available for review.

Organizations have extensive policies and procedures to maintain security and control over data. Still, 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 gain direct data access, it can also circumvent data security measures and clearly breaches general security measures particularly during a fraud investigation. Even if some form of encryption is used, the loss of control over one audit laptop containing critical data can be a major exposure for an organization.

## Analyze large volumes of data quickly

Effective data analytics requires large volumes of data to be processed very quickly. 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 by multiple users with minimal impact on end-user response times.

Because all the data processing is being performed on a server, network traffic is also significantly reduced. Instead of passing entire data files across the network for subsequent processing, only the results are returned to the user's desktop.

Using server technology, you can conduct more comprehensive fraud investigations by analyzing 100% of the transactional data regardless of size, volume, or type; comparing data across disparate systems; and providing effective oversight of the "full picture".

■ [acl.com](http://acl.com)  
[info@acl.com](mailto:info@acl.com)

ACL, the ACL logo, the ACL logo with the text "Data you can trust. Results you can see.", and Audit Command Language are trademarks or registered trademarks of ACL Services Ltd. All other trademarks are the property of their respective owners.

