

This article was downloaded by: [Scheierman, Lark]

On: 7 April 2010

Access details: Access Details: [subscription number 771636584]

Publisher Taylor & Francis

Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



## EDPACS

Publication details, including instructions for authors and subscription information:

<http://www.informaworld.com/smpp/title~content=t768221793>

## How IT Can Help Internal Audit

Dustin Lewis

Online publication date: 30 March 2010

To cite this Article Lewis, Dustin(2010) 'How IT Can Help Internal Audit', EDPACS, 41: 3, 1 – 8

To link to this Article: DOI: 10.1080/07366981003644386

URL: <http://dx.doi.org/10.1080/07366981003644386>

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: <http://www.informaworld.com/terms-and-conditions-of-access.pdf>

This article may be used for research, teaching and private study purposes. Any substantial or systematic reproduction, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.

## HOW IT CAN HELP INTERNAL AUDIT

DUSTIN LEWIS, CISA, ACDA

**Abstract.** Information Technology (IT) and Internal Audit departments have the same business mission, but they can face conflicting responsibilities. The solution must enable IT to provide data without losing confidence, while giving Audit enough flexibility to fulfill the “access to all data” mandate in most every audit charter. This paper describes Audit’s four key data issues, the role of audit analytics in business assurance, and some best practices that can help both IT and Audit manage the key data issues.

**I**n today’s business environment, transaction volumes are growing exponentially and audit groups must be able to examine complete data sets to provide better assurance for their organizations. At the same time, corporate and government regulations for data management, security, and reporting have been steadily tightening. This creates a “push-pull” between those who need the data for business insight and those whose job it is to manage the data. But on balance, businesses do not fail because of minor compliance issues; they fail because management does not have full insight or makes decisions based on poor or incomplete information. Without complete data coverage, major control issues such as revenue leakage and fraud can go undetected—for months and even years.

Information Technology (IT) and Internal Audit (IA) departments have the same business mission, but they can face conflicting responsibilities. IT must safeguard data from violations and errors associated with fraud, control gaps, inappropriate access, and information privacy. Audit, however, needs quick, seamless access to critical business data in order to fulfill its mandate to provide assurance. It’s a significant dilemma, but the solution lies in giving auditors direct access to data in a secure, IT-managed environment. This direct access prevents needless file

### IN THIS ISSUE

- **How IT Can Help Internal Audit**
- **E-Mail Discovery: Latest Cases Impel Public Agencies to Retain Records**

**Editor**  
DAN SWANSON

**Editor Emeritus**  
BELDEN MENKUS, CISA



Taylor & Francis  
Taylor & Francis Group

**CELEBRATING OVER 3 DECADES OF PUBLICATION!**

replication and can minimize the loss of control over mission-critical data.

Before we dive deeper into the role of audit analytics and data best practices, let's explore data access and analysis challenges from an IA perspective. In my experience, Audit faces four key data issues.

## FRAGMENTED DATA TRAILS

Data fragmentation often occurs when auditors store project files on the network, then move on to a different task. When it's time to re-visit that project or help a team member find the right data elements to support a specific analysis, the auditor might struggle to locate the right data file. Faced with potentially tens of thousands of data tables in an Enterprise Resource Planning (ERP) system, each of which may contain a large number of cryptically named data fields, this is a frustrating situation that eats up valuable time and resources. In many cases, it is easier to start fresh with data imports, analysis, and so on than to understand previous work and how to gain efficiencies. This is an unfortunate but common reality that audit teams face when they perform laptop-based analysis in isolation.

## LARGE DATA VOLUMES

Organizations working in industries such as health care, telecommunications, government, finance, and banking will generate enormous data volumes on a daily basis. These files can often be too large for a laptop or the network share drive. Maintaining data in a way that supports efficient processing speeds can also be a challenge, creating delays while auditors wait to complete extracts, downloads, and data processing on their laptops or workstations. In addition, growing network drive storage demands can be costly, forcing IT to establish and monitor quotas.

Many auditors choose not to perform complete data analyses simply because they cannot manage large file sizes and volumes. Whether they are lacking appropriate technical solutions or they have not fully explored these issues with IT, reliance on hit-and-miss

---

**If you have information of interest to EDPACS, contact Dan Swanson ([dswanson\\_2008@yahoo.ca](mailto:dswanson_2008@yahoo.ca)).** EDPACS (Print ISSN 0736-6981/Online ISSN 1936-1009) is published monthly by Taylor & Francis Group, LLC., 325 Chestnut Street, Suite 800, Philadelphia, PA 19106. Periodicals postage is paid at Philadelphia, PA and additional mailing offices. Subscription rates: US\$ 311/£187/€248. Printed in USA. Copyright 2010. EDPACS is a registered trademark owned by Taylor & Francis Group, LLC. All rights reserved. No part of this newsletter may be reproduced in any form — by microfilm, xerography, or otherwise — or incorporated into any information retrieval system without the written permission of the copyright owner. Requests to publish material or to incorporate material into computerized databases or any other electronic form, or for other than individual or internal distribution, should be addressed to Editorial Services, 325 Chestnut Street, Suite 800, Philadelphia, PA 19106. All rights, including translation into other languages, reserved by the publisher in the U.S., Great Britain, Mexico, and all countries participating in the International Copyright Convention and the Pan American Copyright Convention. Authorization to photocopy items for internal or personal use, or the personal or internal use of specific clients may be granted by Taylor & Francis, provided that \$20.00 per article photocopied is paid directly to Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923 USA. The fee code for users of the Transactional Reporting Service is ISSN 0736-6981/06/\$20.00 + \$0.00. The fee is subject to change without notice. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged. Product or corporate names may be trademarks or registered trademarks, and are only used for identification and explanation, without intent to infringe. POSTMASTER: Send address change to EDPACS, Taylor & Francis Group, LLC., 325 Chestnut Street, Suite 800, Philadelphia, PA 19106.

sampling techniques can put the business in a position of risk and minimize essential insight.

## DELAYED DATA ACCESS

IT has numerous responsibilities that can make it difficult to quickly fulfill ad-hoc data requests from Audit. Faced with multiple-week wait-times for source data, auditors may again choose to sample, or spend considerable time negotiating with IT to get working access to the data they need to analyze. It's a situation that can also drain resources and compromise other critical IT duties. Ultimately, Audit needs direct access to critical data or the ability to schedule data extracts during off-peak times.

Delayed access can also affect how Audit completes its work plan—leading auditors to use summarized paper reports, spreadsheets, and sampling instead of testing the actual underlying data. This might mean testing 10–12 items instead of the 20 million transactions that could quickly be reviewed with more sophisticated analysis solutions. If it's too difficult to get the necessary data, or IT has established a complicated relationship or request procedure, auditors will tend to ask for too much or too little data. As a result, IT often pushes back and resents the extra workload. Freedom to obtain data when it is needed suffers when IT wants full control over data access, while Audit requires source data for complete testing. Miscommunication can also lead to Audit receiving the wrong data, and IT ends up repeating the request several times over.

## PRIVACY AND CONFIDENTIALITY CONSTRAINTS

When auditors need source data from sensitive business areas such as payroll or human resources, IT may struggle to preserve confidentiality while delivering adequate records. For good reason, IT is often reluctant to provide direct access to live, operational system data. Security breaches represent a critical risk area for organizations and can result in regulatory penalties, injured reputations, and damage to overall business operations and profitability. It's common practice, however, for auditors to extract critical data and download it to audit workstations or laptops—a significant exposure risk for the organization. As laws continue to tighten and high-profile cases put exposed organizations in the news, data privacy and security is a growing consideration. It's essential that businesses develop appropriate ways to manage security constraints, while still ensuring Audit has the right data to provide detailed operational insight. Fears about data privacy and security regulations can often mean Audit does not receive the data at all, or again, is limited to sample-based testing. The result: privacy and security take priority over true visibility into the health of the organization, and business decisions are made based more on assumptions or historical trends than on facts.

## AUTOMATED BUSINESS ASSURANCE TECHNOLOGY

Despite the numerous data access and management challenges facing both Audit and IT departments, audit analytics provide a powerful solution that can overcome these issues. Purpose-built technology can give IT full security over data sources, while equipping auditors to perform efficient, transparent analysis with access to source data.

An effective business assurance platform should provide streamlined data access, analysis, and reporting for the entire audit group and organization. It should include proven analytics that can be run on-demand or on a scheduled basis. Common analytics include cost-saving tests that look for needless over-expenditures and inefficient purchasing practices, through to a full controls-based approach to testing business processes, such as purchasing, payables, and receivables. The solution should be Web browser-based, and designed to connect directly to data on a scheduled basis and provide detailed reports and exception management to ease accessibility by stakeholders across the organization.

Exception tracking is another essential element of any technical assurance solution. With a closed feedback loop and set procedures for sending, tracking, and following up on exceptions, Audit can ensure that anomalies do not remain unresolved or get lost in the daily shuffle of e-mail and task management. Often exceptions are not escalated beyond an e-mail with an attached spreadsheet. This procedure quickly fails when, for example, someone receives a weekly e-mail with 10–20 exceptions included in a spreadsheet. Within a few months, the receiver of these messages has 15 spreadsheets and 200–300 exceptions. There is no practical way of management ensuring exceptions using this strategy. The ability to track, escalate, and ensure review of exceptions can give an organization unprecedented insight into areas of risk and uncover opportunities to dramatically reduce expenditures (besides simply laying off “x” employees when costs need to be cut).

Most importantly, automated analysis technology must be flexible. Just as each business is unique, there is no one-size-fits-all way to get systems or source data effectively to Audit and other stakeholders. Some audit groups will work strictly with IT to provide targeted data extractions without visibility into source data. Others might allow staff direct access through a data warehouse built specifically for Audit, while others may want immediate access to production data. Regardless, maintaining data security is essential. Audit and IT managers should be able to limit access to specific users and easily change those settings when necessary. Any data access strategy—from direct access to use of extracted text files—should be compatible with a data analysis solution.

With any technical solution, it's equally important to minimize data repetition and redundancy. When many people are using a specific file, it's critical to manage versions and ideally, ensure that a single file copy is available in one location for all appropriate users to access. Technical solutions should also be straightforward and user-friendly. Relying on auditors with specific skill sets can be risky, and can put projects and critical data access at risk if

technical auditors leave the organization or fail to properly document and support their solutions.

Finally, an effective solution will enable the IA team to create and maintain an audit repository that runs within a secure server environment. The repository should consist of data sub-sets, which represent only information necessary for audit analyses. This repository should also include a library to house approved routines, analytics, electronic work papers, documentation of internal controls and regulatory standards, and a clear audit trail for team members to follow. Only administrators should be able to alter analysis routines stored in the library (in order to avoid over-writes, errors, and inexperienced users introducing flawed practices), but audit staff can have read-only access to share work and results.

## SOLUTIONS

Now that we have covered the bases for automated business assurance and data analytics, here are some best practices that can help both IT and Audit manage the four key data issues.

### Fragmented Data Trails

IT can work with the audit group to help them identify not only how to access the data, but also to determine which data best fits a specific business need, such as looking for “ghost” employees in a payroll file. By working as advisors to Audit, IT can save significant time and frustrations for both parties. Auditors who do not have technical backgrounds, for example, might not know what type of data to request, or might ask for a data file that’s far too general. Simple request forms can help auditors to better clarify their needs. Asking questions such as “what do you want to see in the final report?” and “in what format?” can also help ensure that Audit receives the appropriate data with supplemental information, and prevents missing pieces that could be essential for a specific project.

The more information can be gathered up front, the better the data extraction process will be for both IT and Audit. Requests can also be added to data archives and used as templates for future extracts. A strong analytics solution, however, will allow the audit group to access source data directly from a single interface. There should be no need for IT to build data warehouses specifically for Audit, and a secure repository should be established with recurring, automated feeds that can be provided from a single database login triggered automatically from a scheduled server process. Once Audit has been connected to a specific data file, minimal effort should be required to set up access on a daily, weekly, or ongoing basis. The repository should also enable audit managers to restrict access only to specific parties. Even if there are 50 people working with analytics, a strong solution would maintain a single version of each data file that everyone can view.

### Large Data Volumes

To address the challenge of large—and ever-growing—data volumes, best practices promote analytic technology that harnesses the power

of the server. All data processing should take place within the server environment in order to boost speed, ensure data security, and make results immediately available to the intended audience. Servers are designed to process large data volumes and support multiple users with minimal impact on end-user response times.

A strong data analysis solution should also be able to manage near-infinite file sizes. Commonly used spreadsheet software, for example, will hit limits at transaction volumes that large companies routinely reach in a single day. With a server-based solution, there's no need to store data on a laptop or network drive—making the analysis extremely fast. Auditors can quickly look for anomalies among hundreds of millions of transactions and the analytics will not slow the network or individual machines. Picking only the necessary fields from an extensive set of options will also limit the amount of data required for thorough analyses. Scheduling tests to run in off-times, minimizing data volumes with precise filters and queries, and building up offline storage capabilities can further enhance both efficiency and speed. When you have the ability to quickly do “what if” analysis on a large data set you have freedom to discover trends, anomalies, and unforeseen challenges with the same effort previously used in small samples.

### **Delayed Data Access**

Effective data analysis technology will give both IT and Audit multiple ways to tackle secure, timely data access protocols. In one scenario, IT can give Audit access to a secure database that auditors can access whenever they need—either on-demand or through scheduled extracts. Another option is for IT to set up a workflow or process that fits internal security credentials. This workflow can provide to Audit, on a scheduled basis, the appropriate data files. This scenario offers the best of both worlds, because IT does not have to provide data repetitively, on-demand, but still maintains effective control over data distribution and quality.

Best practices also support audit analytics that provide advanced data access, including scheduled downloads during off-peak hours and specialized connectors to specific data types such as eXtensible Business Reporting Language (XBRL), Society for Worldwide Interbank Financial Telecommunication (SWIFT), and Portable Document Format (PDF). This helps prevent regulatory breaches and gives IT greater control over data access procedures. Technical solutions should also have a built-in scheduling function that makes it easy to set up repetitive data access routines without IT intervention. Auditors should find it as easy to schedule data retrievals as they do to set up an Outlook meeting.

### **Privacy and Confidentiality Constraints**

Best practices support analytics with built-in controls that enable IT or management to mask sensitive data such as credit card numbers. Data masking ensures that auditors never see complete numbers, but consistent scrambling techniques still support useful comparisons, matching, and pinpointing anomalies. Keeping data in a secure server environment is another critical element of data

privacy. Customizable security controls should enable audit managers or IT to lock down specific files, results, and areas to certain individuals or groups. The solution should also require logins, and provide tracking and modification notices.

Housing data in a secure, well-managed central repository can also reduce the need for ongoing IT intervention. Auditors can quickly locate and access data necessary for audit projects without requesting time-consuming downloads that may also affect system performance. Standard processes for accessing and updating data ensure that necessary records are readily available, but will not compromise data or network security. Data should be viewed and analyzed in read-only mode, so it cannot be altered or deleted. Eliminating the need for IT to provide data extracts also reduces the length of audit cycles, retains data integrity, and eliminates the burden on IT resources.

Most importantly, conducting analysis tasks within a server environment is the best way to fully safeguard critical data. Security standards can be established for end-user computers such as laptops, desktops, and Local Area Networks, but they are generally easier to circumvent and harder to enforce—even in situations when users inadvertently compromise standards due to error or the desire to work more efficiently. Server environments provide a centralized location where auditors can view full data populations and feel confident that transactions are not accidentally omitted, without breaching information control standards.

While many organizations have security protocols designed to maintain effective and elaborate encryption of laptop data, version control issues can still persist. If more than one person is working on a project, performance can suffer when staff lose track of which version is most current. By default, auditors will usually re-download the data—leading to efficiency and system performance problems if the data must continually be pulled from a database.

## IN CONCLUSION

To remain relevant and to add value to the business, Audit must look deeper into data and reduce its reliance on samples and speculative opinions based on smaller information sets. A PricewaterhouseCoopers survey titled “An opportunity for transformation: How internal audit helps contribute to shareholder value” found that shareholder value is destroyed by strategic and business decisions 60 percent of the time, while compliance issues destroy shareholder value just 5 percent of the time. Looking at the full life of a transaction almost always reveals new lessons that can help strengthen both existing controls and benefit the bottom line. Even the smallest control breaches can point to an ongoing fraud or inefficiency that could waste hundreds of thousands of dollars each year. The business owners also appreciate having detailed information they can use to improve their processes while cutting expenses or maximizing revenue.

The right solution for you should allow IT to provide data without losing confidence, while giving Audit enough flexibility to fulfill the “access to all data” mandate found in most every audit

charter. It's a solution that has worked for many of the world's effectively run companies regardless of size—and it can work for yours.

*As a senior technology consultant at ACL Services Ltd., Dustin Lewis, CISA, ACDA, works with ACL clients to help them understand the benefits of audit analytics technology. He has a background in internal audit and earned the CISA designation in 2004. For over ten years, Dustin has applied audit analytics to gain insight into a variety of industries. He has notable consulting and training experience in government and education. Dustin has significant technical and business experience, and regularly bridges the knowledge gap between a client's IT department and their business leaders. He has worked with audit teams to identify opportunities for saving time and expenses on audit plans. He also developed a consulting practice focused on saving clients money and identifying fraud and waste. As an internal auditor in a bank setting, Dustin used audit analytics to develop an automated continuous monitoring program to monitor nine affiliate banks' ledger accounts. The monitoring tool helped the bank reduce field work and detect problems before they became a crisis. Dustin is a native of Omaha, Nebraska. He has a degree in Business Management with a concentration in Accounting and is a member of the Information Systems Audit and Control Association (ISACA). He received the ACDA certification in 2006. He can be reached at [Dustin\\_lewis@acl.com](mailto:Dustin_lewis@acl.com)*

## **E-MAIL DISCOVERY: LATEST CASES IMPEL PUBLIC AGENCIES TO RETAIN RECORDS**

BENJAMIN WRIGHT

*Norwalk is "at least grossly negligent, if not reckless" in its failure to preserve electronic records.*

—Jane Doe v. Norwalk Community College

### **EXECUTIVE SUMMARY**

Since the adoption of special amendments to the Federal Rules of Civil Procedure in late 2006, the field of e-discovery law has grown more dangerous for public agencies. Recent cases show courts are serious about expecting litigants to possess and be able to find their