White Paper

THE 7 DANGERS OF DOCUMENT-BASED AUDITING

UNDERSTANDING THE DESTRUCTIVE EFFECTS OF DARK DATA ON HIGH-FUNCTIONING AUDIT ORGANIZATIONS

Galvanize

Contents

Executive summary

Using word processing documents and spreadsheets as the primary ways to capture and document audit procedures, results, and evidence is quickly becoming a dusty—and dangerous—anachronism. In today's digital landscape, this approach significantly hinders larger audit organizations in a number of different ways.

In the 1980s and 1990s, large audit organizations moved away from hard copy audit files and working papers because of how difficult it was to share and collaborate on physical files. This was the first major technology transition for the audit profession in many decades.

However, the situation only marginally improved. The problem then became that information gets trapped inside electronic documents and spreadsheets, where it effectively becomes "dark data": impossible to search, reference, analyze, export, report on, or access on mobile devices. This is an issue since all of these are required for large audit teams to support insights and decision making.

It's been some time, and now a second transition is underway. Internal audit teams are moving away from inter-linked documents and spreadsheets, to properly structured databases (accessed through intuitive software interfaces) to unlock the value of audit data—and by extension, unlock the value of the audit organization.

This white paper explores the dangers of document-based auditing, some of the benefits that can be realized by using purpose-built software, and what's needed for making a successful transition over.

The problem with auditing in documents

It is the position of Galvanize that "primary" audit commentary, such as audit analysis, insights, and discussion (see definitions on page 6), should be captured directly into the audit platform where it can be queried. The ability to query information is what makes reporting, exporting, analyzing, sharing, and remotely accessing audit data both possible and seamless.

Documents (and metadata embedded within them) can't be queried, so they should never be used for primary audit documentation like:

+ Core audit work
+ Quality assurance processes
+ Insights and reporting for stakeholders.

However, documents can (and should) be used for supporting audit evidence.

THE DARK DATA TRAP OF DOCUMENT-CENTRIC AUDITING

When the audit community transitioned from physical files to electronic documents, it quickly became unwieldy to track audit status and results among the sea of electronic files. Next, a category of software products for auditors called "electronic working papers" emerged.

At the time, electronic working papers were built to:

+ Centrally store the electronic audit working papers
+ Allow multiple auditors to work on the same audit files while managing version conflicts
+ Allow direct referencing of information back and forth between documents
+ Help reviewers follow the auditor's work, and provide comments and coaching
+ Link commentary and points of reference from one document to another.

With these benefits, legacy audit management software solutions built on electronic working papers were a critical advancement in the evolution of audit processes and execution at that time.

In the current digital environment though, these systems have stunted the growth of audit value and innovation due to an unforeseen—but major—blind spot. The fundamental problem is that key audit information is effectively turned into "dark data," trapping important insights inside these documents.

What is dark data? *Gartner[1] defines dark data as "the information assets organizations collect, process and store during regular business activities, but generally fail to use for other purposes (e.g., analytics, business relationships, and direct monetizing). Similar to dark matter in physics, dark data often comprises most organizations' universe of information assets. Thus, organizations often retain dark data for compliance purposes only. Storing and securing data typically incurs more expense (and sometimes greater risk) than value."*

1 Gartner, IT Glossary. http://www.gartner.com/it-glossary/dark-data

7 DANGERS OF DOCUMENT-BASED AUDITING

The key problems created by the document-based approach to audit management include:

1 **Dark data gets trapped inside the documents or spreadsheets.** Data intelligence can't be efficiently accessed by reporting systems, data analysis tools or mobile devices, severely impairing the value of that information in delivering key business insights.

2 **Documents don't protect data integrity.** Embedding audit process metadata (i.e., tick marks, review notes, auditor commentary, inter-document links and references) into document files creates significant data integrity risk. Systems that rely on deep document integration are therefore prone to data loss when files are corrupted, if they're edited in conflict by disparate users, or if they're moved between locations that break references and relationships. This also causes slow performance, as documents simply can't perform at the level of database-driven systems.

3 **Information inside documents or spreadsheets can't inherently maintain its relationships to other information.** Again, since documents are not databases, there is no mechanism to create and maintain a relationship between data in different files. Hyperlinking and other document-embedded features are therefore inherently unreliable.

4 **Rolling forward audits is difficult and very manual.** When primary audit documentation is captured in documents, it is impossible (or very dangerous) to update programmatically. When rolling an audit forward, all data must be updated manually.

5 **Exporting and archiving outside the software is impossible.** Hyperlinking information inside and between documents—referred to as "deep linking"—necessitates document-embedded metadata, with references stored in the software system. Since a link from inside one document to another depends on this externally stored reference, it is impossible to archive or export an audit project outside the software without breaking those links.

6 **Dependencies cause software version conflicts and difficult upgrades.** As Microsoft® Office and other document editing software is updated and file formats change, integration dependencies often break the compatibility of the audit software. This leads to situations where, for example, a new Office version forces an upgrade of the audit software or changes the embedded metadata (again causing data integrity risks). Even in the best case, upgrades require rigorous testing, which causes lengthy delays in upgrade implementations.

7 **IT burdens.** Creating and managing document-embedded metadata requires that these legacy audit software systems include a locally installed application or complex web browser plugin. Because they are hosted individually on local machines, these applications create significant IT administrative burdens, including high-maintenance installation rollouts and upgrades, and compatibility issues.

Imagine if **Amazon.com** saved their records of every sales transaction in thousands—or millions—of documents and spreadsheets. It would be near impossible to find the answers to important questions like "What were total sales?", "What are our most popular items?" or "What should we recommend to shoppers next?" without armies of people compiling the related information manually. Fortunately, it is possible for companies like Amazon to answer questions like these in an instant because that information is stored in databases that are searchable, reportable, and exportable.

Why treat differently information captured in the process of conducting an audit?

It's not you, it's audit technology

Understanding digital audit evidence = understanding the need for change.

From a core audit methodology standpoint, critical audit documentation falls into two broad categories:

1 **Primary audit analysis and insight:**
This is any information that is the original thought of the auditor that would end up in an audit report, like their analysis and commentary about the procedures performed, why they were done, the results, conclusions, etc.

2 **Supporting audit evidence:**
The artifacts that are acquired during the audit that directly evidence what led the auditor to their conclusions.

For the sake of illustration, consider a court proceeding: while exhibits and evidence are, to every extent possible, unmodified from when originally collected, lawyers also prepare commentary on the exhibits and evidence. The commentary is subject to detailed interrogation in search of insights that will illuminate the truth, but the supporting evidence and exhibits remain as pristine as when discovered.

You can think of supporting audit evidence in the same way as court evidence. Supporting audit evidence should be gathered and secured as pristine artifacts, unmodified in any way, to maximize defensibility. The commentary of the auditor can be considered like legal commentary. The auditor's commentary should be treated as primary audit analysis and insight.

This primary audit analysis and insight should only ultimately live in a structured database system—to give the advantage of infinite "query-ability." As much as it's critical not to contaminate the evidence, it's just as critical not to lock away the analysis and commentary.

A properly structured audit management software system ensures auditors operate according to these conventions, so stakeholders can glean maximum insight by interrogating the audit commentary and analysis, with the assurance of supporting audit evidence.

How to avoid dark data

Dark data is created when auditors—and, more specifically, the auditor's technology toolset—allows primary audit documentation to be captured in files that isolate that information from query-ability and obscure it from audit logging.

There are three key areas you can address to make sure that your insightful audit work does not slip into becoming dark data:

+ **People:** Develop and communicate a "tone from the top" for your entire audit team. Confirm that internal audit is undertaking a simple but transformative step in its ability to deliver insight with agility and flexibility. By not primarily auditing in documents, you can respond at the speed of the organization.

+ **Process:** Incorporate procedures into the core audit methodology so that all auditors understand the two categories of digital audit documentation; that audit working paper preparation is being conducted accordingly, and that quality assurance processes are aligned to review for the same.

+ **Technology:** Protect your auditors by selecting technology wisely, and enacting a workflow that discourages primary audit information being documented in dark files and disables key metadata from being embedded in those files.

Dealing with the challenge of change management

If your audit organization is trying to change processes to eliminate dark data, you may face the challenge of change management. This is most challenging if you are a large audit organization; it's typically more difficult when migrating from an environment that encourages document-embedded data and metadata, rather than an environment using no audit management technology at all. However, the transition is well worth the investment.

With insight from hundreds of audit working papers technology implementations, the critical success factors in overcoming change management challenges are:

+ A vocal recognition and understanding of the problem at the leadership level.
+ Identifying methodology champions at the manager level who consistently reinforce the fresh approach and champion oversight of the removal of dark data issues throughout the audit review and sign-off processes.

WHY CHANGE? KEY BENEFITS FOR INTERNAL AUDIT

Investing in the near-term change management necessary to shift your organization away from primarily document-based auditing and towards audit management software drives key benefits.

+ **Improved productivity of audit fieldwork**. Auditing software puts clear structure around audit procedures to efficiently guide your staff and avoid confusion.
+ **Much higher consistency of approach and quality between audits**. Lifting the work out of documents and into the audit system ensures that a structured methodology is followed.
+ **Elevated quality of audit insights**. Through the ability to report and analyze audit information across projects and teams with advanced tools, you can identify higher-quality, higher-level, and deeper root-cause insights.
+ **Easy expansion of the breadth of audit insights**. Your auditors can instantly answer stakeholder questions and provide expanded insights when data is able to be fully queried.
+ **Faster insight delivery**. No need to wait until quarterly or bi-annual audit packages are prepared to compile and deliver results.
+ **Improved ability to present high-impact reports**. Use beautiful, interactive dashboards and visualizations to present insights, rather than manually compiled reports.
+ **Easier, less "invasive" audit roll forward**. One-click roll forwards that do not require invasive updating of embedded document links.
+ **Generally enhanced audit automation**. Enables "edit once, updated everywhere" workflow; automated audit report creation; and easy cloning, roll forward, and reuse of audit work.

This same transition also relieves **administrative and IT-related burdens for the organization**. More benefits include:

+ Avoiding data integrity risks resulting from using files to store embedded "non-document" metadata.
+ Getting rid of the need for PC installations, upgrades of client software, complex browser add-ins, as well as the associated version incompatibility conflicts.
+ Making data more exportable and transferable
+ Ensuring all data is accessible on any device, including the ability to work with audit information in native mobile applications.

Do you have a dark data problem? Let us help you.

Are you suffering from any of the following document-based auditing symptoms?

- ❑ I spend excessive amounts of time piecing together manual reports.
- ❑ I'm unable to apply analytics to audit commentary to illuminate valuable trends.
- ❑ I'm unable to quickly adapt to changes such as regulatory updates or emerging risks, or cascade changes through my audit programs.
- ❑ I have "zero" to "blurry" oversight over my team's audit project statuses and what may be blocking them, which means I can't unblock obstacles.
- ❑ I lose too much time to upgrades that cause everything to break.
- ❑ I'm frustrated with bloated audit documents that often get corrupted.

If any of the above sound familiar, you need to ask yourself: If your audit committee or executives decided your organization needed to invest in a department to do things better, why are you putting yourself in the position of having to go through so much trouble to surface these insights?

Internal auditors do a tremendous amount of work capturing important thinking and evidence, uploading status updates, and so much more—but is all that effort going nowhere? Documents should not be databases. Instead, use technology that captures audit information in a way that is structured according to database methodology so that you can report, analyze, and collaborate using this goldmine of business intelligence. Don't bury your brilliance in a way that you can't report on and share.

You're doing way too much important work to lose that value to a technology black hole.

If you think your data has gone dark, call us for a free assessment. Stop losing time to upgrades that break, corrupted and bloated documents, syncing issues, manual report-building, and unearthing trapped intel. We'll show you how the right technology can help you bring your data, your insights, and your audit team's value into the light.

IF YOU'RE NOT ALREADY A GALVANIZE CLIENT, CALL US

In pursuit of audit excellence, Galvanize's working papers software does not allow embedding primary audit information into document files. Our audit management technology is designed to avoid features or functionality that allow inter-document links and references. We coach teams and customers to avoid capturing primary audit work in document files. Our approach eradicates dark data from audit projects, which creates substantial opportunities to elevate the quality of audit insights, the breadth of audit insights, the speed of insight delivery, and the impact of internal audit on every organization.

About the author

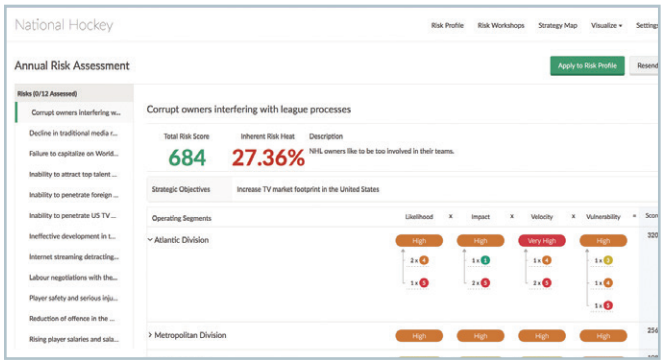
DAN ZITTING, CPA.CITP, CGMA, CISA, GRCA

Dan Zitting, chief customer experience officer, is dedicated to the advancement of cloud and "big data" technologies for helping corporations and governments perform better while operating with integrity. Dan has been recognized with multiple awards, including CPA Practice Advisor Magazine's "40 under 40," Business in Vancouver's "Top 40 Under 40," The IIA's "Emerging Leaders," BCTIA's "Team of the Year" and GRC 20/20's "Technology Innovation" awards. He is regularly quoted and covered in publications including The Wall Street Journal, CFO Magazine, Bloomberg, Reuters, The Street, CNBC and more.

Prior to Galvanize, Dan spent 10 years in professional services with the IT Risk Advisory Services practice at EY and as a Partner and co-founder at Linford & Company LLP, a provider of GRC consulting services to clients across North America, Europe and Asia.

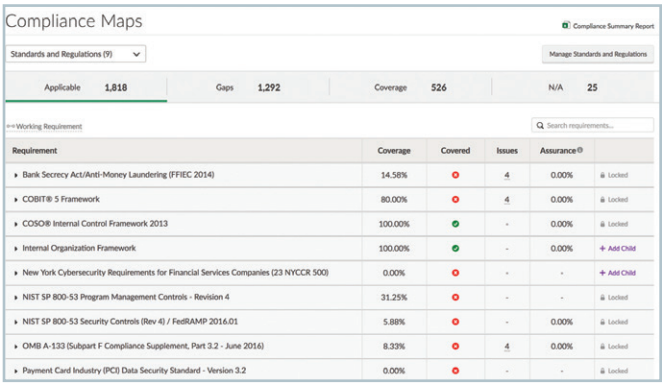
While building his firm, Dan developed a software platform for use by clients, which ultimately led to founding Workpapers.com, the first truly cloud-based audit and compliance management system in the market. Under Dan's leadership, Workpapers.com was acquired by Galvanize in late 2011, combining the power of cloud collaboration and big data analytics under one market-leading brand.

Dan holds a Bachelor of Science from Colorado State University and a Master of Science from the University of Notre Dame.



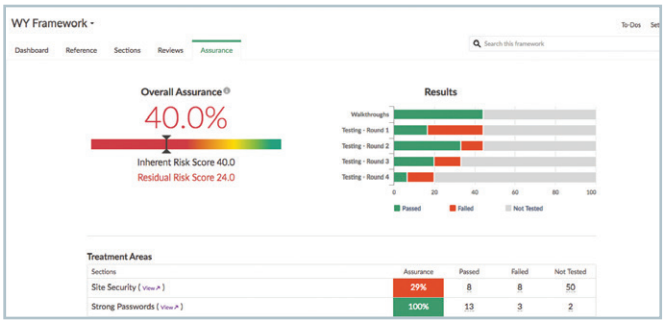
Risk Workshops

Collaboratively assess risks as a leadership group from a central view in real time, and talk about the impact to strategic objectives.



Compliance Maps

Keep current with the latest regulations or industry standards for which you're providing assurance, and map them to the controls that make you compliant.



Frameworks Assurance

Get a bird's eye view of your process-risk-control activities collectively providing assurance across strategic risks and compliance obligations.

About Galvanize

Galvanize builds award-winning, cloud-based security, risk management, compliance, and audit software to drive change in some of the world's largest organizations. We're on a mission to unite and strengthen individuals and entire organizations through the integrated HighBond software platform. With more than 7,000 customer organizations in 140 countries, Galvanize is connecting teams in 60% of the Fortune 1,000; 72% of the S&P 500; and hundreds of government organizations, banks, manufacturers, and healthcare organizations.

Whether these professionals are managing threats, assessing risk, measuring controls, monitoring compliance, or expanding assurance coverage, HighBond automates manual tasks, blends organization-wide data, and broadcasts it in easy-to-share dashboards and reports. But we don't just make technology—we provide tools that inspire individuals to achieve great things and do heroic work in the process.

Learn more about what you can accomplish with Galvanize

1.888.669.4225 | **wegalvanize.com** | **info@wegalvanize.com**