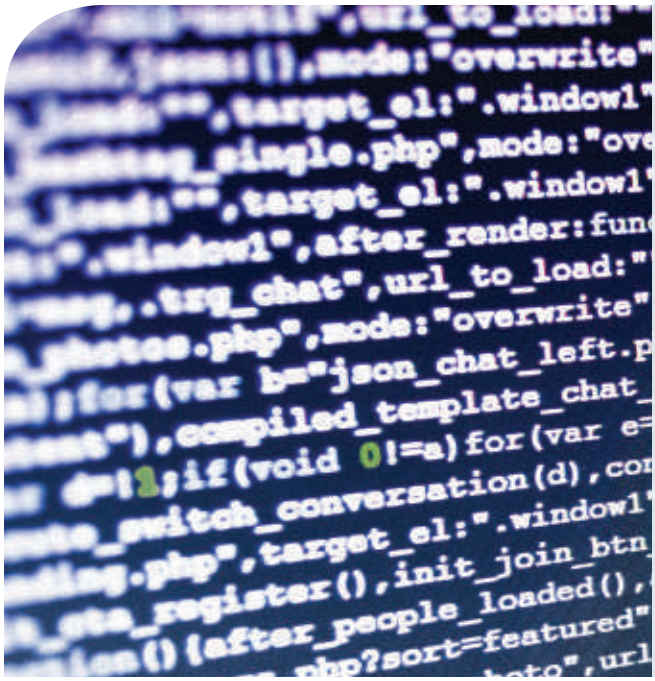
While organizational analytics can yield powerful insights, they may also be a source of risk.

Jane Seago



Behind the Data

Businesses are having a love affair with data analytics. The potential to unlock secrets hidden in the vast quantities of data generated daily makes the technology almost irresistible. And why not? Tools enabling the organization to uncover data patterns that reveal how to implement efficiencies, make better decisions, increase agility, identify untapped market niches, and appeal more viscerally to customers can be extremely valuable.

Internal audit is no stranger to using data analytics to fulfill its responsibilities to the organization. But not only does internal audit use data analytics itself, it also is called on to review the data analytics use of the business units. Such audits are performed because of the growing realization that insights are not alone, hiding in the data; risk lies there as well. And where there is risk, there is a need for internal audit.

"The same types of questions we would consider for other processes in terms of where things could go wrong apply to data as well," says Judi Gonsalves, senior vice president and manager, Corporate Internal Audit, with Liberty

BEST-BACKGROUNDS / SHUTTERSTOCK.COM

TO COMMENT on this article,
EMAIL the author at jane.seago@theiia.org

> The same types of questions we would consider for other processes ... apply to data as well."
>
> Judi Gonsalves

Mutual Insurance Group in Boston. And with ever-growing volumes of data on hand, and further organizational dependency on that data, those questions become more and more important to ask.

ASSESSING THE RISKS

The possibility of things going wrong explains why internal audit should start, if it has not already, reviewing the use of data analytics in the organization. More than 70 percent of chief audit executives (CAEs) surveyed in The IIA Audit Executive Center's 2018 North American Pulse of Internal Audit research indicate that their organization's net residual data analytics risks are "moderate" to "extensive." But what, exactly, are those risks?

A risk cited by several experts can be summed up in the familiar phrase, "garbage in, garbage out." If the data being analyzed is inaccurate, incomplete, unorganized, dated, or siloed, the conclusions drawn from it can hardly serve as the basis for a winning business plan. "We worry most about the completeness and accuracy of the data pulled together and upon which management may rely," notes Katie Shellabarger, CAE with automotive dealer software and digital marketing firm CDK Global in suburban Chicago. "Management may take the information prima facie and not know that the data is wrong."

> The more data the organization has, the more incentive it may provide malicious actors to hack into it.

Tom Rudenko, CAE with online business directory provider Yelp Inc. in San Francisco, echoes this concern about data quality. "Our audits evaluate the risks around the completeness, accuracy, integrity, and security of data," Rudenko says. "For example, if a data warehouse is part of the data analytics process, we look at risks and controls around the entire path of the data: the sources of the raw data, the methods and technology around transferring the data to the warehouse, the controls over the warehouse, and the transfer to the end user." Rudenko explains that, in this example, if there are errors or problems with the data at any point along this path, then the end result may be flawed and any decisions or conclusions relying on this data may also be flawed. "If there are any weak links along the journey to the end user, then the entire chain may break," he adds.

Alternatively, the data may be sound, but the algorithms used to analyze it flawed. They may contain an ancillary function, such as an edit check, that is doing something other than its intended purpose, without the business unit being aware. This anomaly may not influence the result. But then again, it might.

In addition, questions should be asked about the data collection process itself. Was it ethical? Is the data being used for the purpose for which it was collected? Was it collected in a way to provide objective results or to prove a point?

"We have to be careful of bias in how we, as auditors, test," says Charles Windeknecht, vice president of Internal Audit with Atlas Air Worldwide in Purchase, N.Y. "We cannot let our initial impressions drive our subsequent actions. If we are unduly influenced by an early fact, we may go down an incorrect path, getting a result that appears accurate while not realizing we are unintentionally overlooking other data."

Nearly 75% of CAEs report their organizations' data analytics maturity level as less than "established," according to The IIA's 2018 North American Pulse of Internal Audit survey.

GETTING STARTED

CAEs and internal auditors just beginning to audit the organization's use of data analytics may welcome some words of wisdom to ensure favorable results. The experts offer several suggestions:

- Consider the advantages and drawbacks to building analytics capability in the existing team versus acquiring talent.
- Engage with management, especially in the planning process. "If they are not involved, the process may get started, but it is less likely to be sustainable," Rudenko says.
- Start small. Understand the process and break it into manageable, auditable parts.
- Have realistic expectations. While the internal audit function may hope to spring from level 1 to level 4 with regard to its ability to use data analytics effectively in the audit process, the reality is that it takes a lot of effort just to go to level 2. The level of internal audit's understanding and capacity to use data analytics does influence how to effectively audit a control process with heavy reliance on similar routines.
- Take the time to work through the false positives that are likely to arise during the initial execution of the audit testing routines.
- Look for a win. "Start by auditing candidates, or processes, where you are likely to gain success," Windeknecht advises, "then build on that success."
- Look to local IIA chapters for shared experience/expertise and libraries of data analytics routines and audits of data-analytics-driven control processes. Some have formed discussion groups specific to data analytics.
- Have the end game in mind. "Know who is relying on the data and what they are using it for," counsels Robert Berry, executive director of Internal Audit at the University of South Alabama.

"If there are any weak links along the journey to the end user, then the entire chain may break."

Tom Rudenko

"Management may take the information prima facie and not know that the data is wrong."

Katie Shellabarger

Other risks related to data analytics are many and varied. The more data the organization has, the more incentive it may provide malicious actors to hack into it, thus compromising security and privacy. In addition, change management techniques and monitoring/maintenance of who has access to the data are causes for internal audit attention.

PROVEN METHODOLOGIES

When faced with a diverse and complex range of risks, tried and tested audit approaches often yield the best results. Take, for example, the timing of data analytics-related audits. Windeknecht indicates that his team's audits are generally driven by the annual plan, which is updated quarterly. "However, if there's a process that's identified as risk-driven, such as analytics, we will audit that process and test those controls as an addition or replacement to the formal plan."

Often, the timing of data analytics reviews depends on the nature of the data. "If the data is critical to the production of our financial statements, then it gets reviewed as part of the ongoing Sarbanes-Oxley process," Rudenko says. "If the data relates to operational, technical, or regulatory risks, the frequency of our

reviews is factored into our audit planning process."

But scheduling is not the only area where established practices can prove beneficial to review of analytics use. The techniques used to conduct the audit can be relatively standard as well. For example, Robert Berry, executive director of Internal Audit at the University of South Alabama in Mobile, asks the department he is auditing what reports it generates. "Depending on the source of the data and how it is used, we may need to look at it, because management may be making critical decisions based on it," he says. Berry's team relies on a structured approach to audit the data analytics process and reuses approaches that have worked well in one department for other departments.

Personnel-related controls are critical in relation to analytics, particularly management oversight and user education.

"I've seen audit teams reach completely inaccurate conclusions because they went down the wrong path early in testing."

Charles Windeknecht

A traditional approach applies also to the controls recommended to address any findings: input controls (the data's completeness, accuracy, and reliability), processing controls (reconciliation of changes made to normalize/filter the data), and output controls (accuracy, based on inputs and processes). Consider, for example, the data warehouse, which supports data analytics. It has teams of personnel dedicated to operating and maintaining it, and features pipelines from the sources of data to the warehouse and from the warehouse to the end users. In this scenario, Rudenko suggests assessing whether or not:

- Personnel have the necessary expertise to ensure the completeness, accuracy, integrity, and security of the data.
- Processes and controls surrounding the use and security of data are clearly documented and communicated.
- Appropriate and relevant access and change management controls are in place and tested for operating and design effectiveness.
- Changes to the control environment and supporting databases are tracked and monitored.
- The analyses are supported by built-in quality and effectiveness checks to ensure they (and the data) mirror the changes and evolution of the business.

Personnel-related controls are critical in relation to data analytics, particularly management oversight and user education. Shellabarger points out that if users have flexibility to create their own reports/analysis, they need to know how to use the tools correctly and how to evaluate the inputs and outputs. "Essentially, they need to be able to address the completeness and accuracy issues related to using data and tools," she says.

THE FINER POINTS

While proven methodologies may come into play throughout the process of auditing the business units' data analytics use, that does not mean such audits do not present their own unique challenges. As with every audit, there are subtleties that must be recognized, understood, and resolved.

For example, Windeknecht points out that even the apparently basic exercise of identifying data analytics is far from straightforward. "What do we define as data analytics?" he asks rhetorically. "Business units are doing analyses in different shapes and forms, using different algorithms and basing

Nearly all companies say they have implemented big data analysis, are in the process of implementation, or are considering it, according to research and analysis firm Stratecast.

their analyses on different assumptions." Risks can arise when the internal auditor or the business unit itself incompletely or incorrectly understands or agrees on such foundational issues. "Are the assumptions still valid?" he continues. "How do you perform integrity checks? When was the most recent review of the algorithm? How does one data event influence subsequent activity?"

Internal auditors make a big mistake if they do not validate key assumptions with facts (i.e., confirmation of key data points and the underlying assumptions) before continuing with testing. "I've seen audit teams reach completely inaccurate conclusions because they went down the wrong path early in testing," Windeknecht says. "The root cause for the error was not sufficiently validating assumptions and initial results. The issue is a huge hit to the integrity of the testing and audit process. The issue is not one you want to confront during the reporting phase of the audit."

Berry points to challenges even in knowing exactly what to audit. He explains, "On a micro level, when you look at a specific department, you have to understand the objectives of the deliverables/reports, the sources of the data, and the distribution of the data." It is important to review the process undertaken to produce reports: how the data changes through the cycle and how the changes are accounted for. He advises framing the audit around "reconciling base data to final output."

On a macro level, it is important to prioritize. "Every department has data it is analyzing and using to produce a result, every department has goals and objectives, and every department has to report on how it performs against those goals," Berry says. "You have to work with the departments to identify reports used in management's decision-making process. That will help you know which activities to review and why."

And, finally, even the most thorough, meticulous audit will fail if its findings cannot be explained in a way that resonates with the business unit that has been audited. Internal auditors must consider the learning modalities of their audit clients when discussing the findings; people hear, see, and experience things differently. While the natural inclination may be to simply hand over a written, text-heavy report, it may be more effective to use visually appealing, concise images in support of the text. A verbal presentation — in support of the written report — that includes concrete examples of the findings or the risks that may accompany the findings is also likely to make a more lasting impression. This gives clients multiple ways to absorb and understand the recommendations, based on the way they process information.

"You have to understand the objectives of the deliverables/reports, the sources of the data, the distribution of the data."

Robert Berry

MIND THE DETAILS

The old saying that "the devil is in the details" is particularly apt for reviewing data analytics. And, as with many aspects of internal auditing, a dose of healthy skepticism is helpful. Says Gonsalves: "We cannot assume that just because information comes out of a system, it is automatically correct." IA

Auditors make a big mistake if they do not validate key assumptions with facts before continuing with testing.

JANE SEAGO *is a business and technical writer in Tulsa, Okla.*