Trends, Challenges and Strategies for Effective Audit in a Rapidly Changing Landscape

Traditional audit is a typically retroactive activity that identifies risk in running operations and proposes solutions. The common wisdom is to not fix what is not broken. So, what exactly needs fixing in audit? How much of the need to change is real and how much is hype? Perhaps focusing on some important elements for effective audit—namely the time element, competence, analytics and automated tools, and agility—can help answer these questions.

The Time Element

One aspect of the modern business environment is frequent and often radical change driven by technology, demand, competition and regulatory developments. Businesses and their management, systems, procedures and people need to respond in time to these challenges. However, a timely response was also required in the past. What is different now is the pace of change and, perhaps, the severity of the consequences of not keeping up. Audit needs to keep up with this pace to be useful by providing timely assurance.

Today, data are often available in real or almost real time and, in theory, both management and audit should be able to quickly collect and analyze data for their respective needs, e.g., data verification, checking for errors and abnormalities. This is often referred to as continuous auditing (CA). However, data availability does not by itself mean that changes in audit are warranted. For example, even when one has real-time data and technology allows for the analysis of the data in real or near-real time, time may be needed to filter out noise and identify trends, i.e., one may need to accumulate data over a longer time period to draw conclusions. Additionally, if the reaction time is months, then it makes little sense to require a detection time in minutes or hours. In short, risk, business needs and cost/benefit determine the meaning of timely: Just because data are available in real time does not mean that processing or response need also be real time. There have been cases where auditors are pressed to finish fieldwork in a few days, when just scheduling a closing meeting can take several weeks. The time element is relevant to the entire audit process, not just fieldwork or aspects under the auditor's exclusive control.

That said, there are cases where immediate detection and response are necessary, for instance, security breaches. However, this is not the primary function of audit, nor does the organization rely on audit to deal with security breaches. Audit is more likely to evaluate the adequacy of controls than to actually detect breaches. This is a bigger-picture/longer-term view than operational activities. In other words, audit is more concerned with what should be in place to detect and defend against

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2nVEcvf

Spiros Alexiou, Ph.D., CISA, CSX-F, CIA
Has been an IT auditor for a large European enterprise for the last 12 years. He has more than 24 years of experience in IT systems and has written numerous sophisticated computer programs. He can be reached at spiralexiou@gmail.com.

breaches and how well it is working. This requires a further level of abstraction and testing and is different from working on a specific breach or breach attempt.

Timeliness has always been an important factor, and the nature of audit does not mean that all audits have equal time requirements or that they need to be in real time. And the ease of collecting and analyzing data is not a given.

Competence

One element of audit that has changed, however, is competence requirements on auditors, particularly IT auditors. The diversity and complexity of IT systems creates serious competence demands on auditors. In the breach example previously discussed, the auditor is required to understand all possible ways a breach can occur and what needs to be done to conduct an effective audit. The auditor may be less familiar with a specific product than the administrator who uses it daily; nevertheless, the auditor needs to have detailed knowledge to address the important risk and ask the right questions. Again, competence is required in all standards and is directly related to effectiveness to avoid "drive-by" audits that bring little value. So, qualitatively we have no change. Quantitatively, though, the change in demands placed on auditors is significant, as auditors must keep pace with technological change without being involved in day-to-day operations.

> "THE DIVERSITY AND COMPLEXITY OF IT SYSTEMS CREATES SERIOUS COMPETENCE DEMANDS ON AUDITORS."

This, in turn, means that first, IT auditors should ideally have operational backgrounds (though they hardly need to be familiar with the quirks of any new system employed by the organization). Second, they must keep up with developments. The first requirement is addressed via proper personnel selection for the audit function, ideally from within the organization, and the second by continuous education of the auditors.

Analytics and Automated Tools

There is much talk (and fear) that "intelligent" machines will replace all kinds of professions; indeed, this has been happening since the 1990s. However, these earlier machines were not "intelligent"—they simply could perform routine tasks such as mathematical operations more efficiently than humans. This is changing now because machines can learn and exhibit what we identify as intelligent traits in humans, the most important of which is the ability to learn, with or without supervision.

For instance, the Alpha0 engine learns from results (reinforcement learning), much like a child learns from the outcome of touching a hot plate. The main driver behind such intelligence is deep neural networks. However, neural networks have a significant drawback from an audit perspective: They cannot simply explain their results. For instance, a neural-based firewall can be very effective in filtering out malicious packets, but it cannot explain why. In addition, reinforcement learning is not always practical: To learn chess[1] or Go,[2] the program can afford to lose many games while learning. It is not practical to bankrupt many enterprises to learn about good and bad management practices. Furthermore, the games previously mentioned have clearly defined win/lose/draw conditions, which is not the case for businesses, where record profits at one point may be an interim result of disastrous decisions that eventually lead to bankruptcy.

Hence, for audit purposes, neural nets is likely to be an exploratory tool rather than a confirmatory one. Other artificial intelligence (AI) tools such as clustering, which identifies classes of "similar" behavior, or case-based reasoning, which assesses "closeness" to known cases, can also be useful in fraud detection, for instance. An excellent understanding of the business aspect in question (domain expertise) is essential to use these tools[3] (i.e., assigning numbers to different attributes). Indeed, it would be hard to catch an interesting exception if one does not know what interesting means or what interesting traits might involve. Neural nets that can catch interesting exceptions do

not explain why (and would also not explain their possible failure to catch an emerging trend remote from their training).

Nevertheless, even without AI, new technologies are also often seen as competitors to audit: Since the data are available, why not program a system to do all the checks that auditors do? This is also seen as another attractive cost-cutting proposal. The system checks everything and management can rest assured. Continuous monitoring (CM) is defined as:

> *...a non-emotional, never tiring automated 'monitoring agent' inspecting, in real time, verifying adherence with enterprise policies, authorizations, proper sequence, correct time frame, in the right location/region, and so on*[4]

It is a good idea, especially for mature systems and environments that obviously strengthens the control environment. Indeed, some argue that CM could have detected and prevented the Worldcom scandal.[5, 6] There is no reason for auditors not to embrace any tool that helps them perform their function in a more effective and efficient manner. However, replacing audit with continuous monitoring is another idea destined for failure, for a number of reasons.

First, audit is about risk. Risk is almost never static but evolves with the business and its environment, including customers, authorities, competitors and employees. Not checking the effectiveness of such systems is like relying exclusively on a sturdy fence for the security of a military installation.

Technologies alone do not identify risk, and everyday checks will typically miss risk they were not programmed to identify and mitigate. Even AI will not identify risk if relevant information (e.g., fields) is missing from the data. It takes domain experts to understand risk and how to prevent and detect it, and their input is also needed to revise risk.

The risk-handling process typically starts by identifying, classifying and dealing with the most important risk first, rather than all possible risk. An analogy would be a fence, where initially one would focus on closing gaps or holes in the fence because these represent the greatest risk (easiest way to intrude). Once this is done, a reevaluation of remaining risk and its severity would be in order and would result in further mitigating measures, such as taller fences and patrols, among others.

System checks are, of course, essential, including computer-assisted audit techniques (CAATs). However, it is important to distinguish first-line-of-defense activities, which should be a part of normal audit operations from audit-type activities. Detecting and responding to exceptions and irregularities should be part of everyday operations. Audit's function is very different: It is to verify that the controls in place are adequate and work and to possibly detect exceptions and irregularities that have not been detected or addressed. As such, audit is a further safety net whose responsibilities are well beyond standard, everyday checks, such as predefined tests performed routinely via automated tools.

"TECHNOLOGIES ALONE DO NOT IDENTIFY RISK, AND EVERYDAY CHECKS WILL TYPICALLY MISS RISK THEY WERE NOT PROGRAMMED TO IDENTIFY AND MITIGATE."

For example, a fraud case was identified that was missed by everyday operations that did examine but did not correlate the same information. Once this scenario was identified, checks were implemented as part of everyday operations to thwart this method. This can also occur for vulnerabilities that may initially go undetected by everyday operations. In other words, audit's function does not compete with existing routine automated tests but is to access their effectiveness and efficiency and to propose extensions to these tests and/or new tests that will cover identified remaining risk.

Second, even the most sophisticated system can make mistakes, and these can be errors that could be glaringly obvious to a human, typically with serious consequences, especially in view of current legislation in many countries. Anyone, including

sophisticated systems, can still err for a variety of reasons including programming and/or logic errors, quality of data, and user input. Complex programs can make error detection especially problematic.

Third, even the most sophisticated system needs data to make decisions. These data may be doctored or altered, perhaps even by accident or malfunction, to reach an inaccurate conclusion. Hence, data reliability is an issue, as automated systems without built-in audit capabilities (capabilities that come with their own risk) are ultimately under management control, with financial data being a well-known target. This again is not new and has happened as early as the late 1960s and early 1970s; that is, in a time when "Only a select few knew how to operate [computers] and everyone believed in what the computer came up with and printed out."[7]

In the same example (the Equity Funding Corporation scandal), audit was also fooled because systems were under management control:

> *When auditors attempted to confirm receivables via phone calls to customers, switchboard operators at Equity Funding would simply connect the calls to employees who would subsequently confirm the balance information.*[8]

Similarly, "auditing around or through the computer"[9]—that is, using computer outputs or computer systems in testing both controls and transactions—may be inadequate in the modern day because, although it is much easier to rely on computer systems to do the work, the reliability of these systems must also be independently established. This is not always easy to do because computers are complex systems. Embedded audit modules (EAM) may help; however, assuming their integrity, it must be kept in mind that a) they will be only as helpful as the information they collect and b) they could run into performance problems, especially if they adopt a "let's collect everything" philosophy. Typically, these modules are made by the manufacturer, who may not have as clear a view of critical audit information as the people actually running the system or have the needs of auditors in mind. As a result, the need for testing and critically examining computer output rather than having blind faith in the infallibility of the computer results will remain strong. Reasonableness of results, comparing results to one's rough estimates and investing the effort in understanding why the computer gives these results are needed on the part of the auditor.

The emergence and proliferation of automated tools has implications for auditors: On the one hand, auditors have more and better tools to be more effective in their work, including aspects of more or less standardized work such as reporting (although reporting is not exactly a routine task, it can be standardized much more easily than fieldwork), where one should get all the benefits of automation for routine tasks. On the other hand, these developments increase the competence and effectiveness requirements made on auditors, who must be able not only to use new technologies, but also to understand how they work, what could go wrong in their results and how to check them.

> "EVEN THE MOST SOPHISTICATED SYSTEM CAN MAKE MISTAKES, AND THESE CAN BE ERRORS THAT COULD BE GLARINGLY OBVIOUS TO A HUMAN."

In some cases, audit departments have started looking for an "analytics tool." In one case, this tool had already been purchased by the audit department more than 10 years prior, but no one was using it. This is the wrong approach. The right way is to first determine the analytics needs, then ask how to best address those needs.

For instance, a common IT audit theme is to verify user access; that is, that only authorized people had access to the IT systems. This entails comparing the "as is" situation—for example, the Unix, Linux, among others, password file with the "as should be" situation, which is basically a list of authorizations, for instance via an identity management system (IDM). A general program to do this comparison, developed in-house by an auditor and given a

graphical interface to be able to handle multiple "as is" file formats, proved much more useful than any external tool.

> "THE MORAL IS THAT NO TOOL WILL TELL ONE WHAT ONE NEEDS TO CHECK OR RECONCILE, AND THIS IS NOT LIKELY TO CHANGE IN THE NEAR FUTURE."

Similarly, checking shop operations such as returns, discounts and collections, among others, and other technically complex cases was again done via in-house software and was proven to be much more effective than trying to "fit the data to an external program." In fact, the team that operated the external program lacked the domain expertise and concluded that "your data is not good enough for our program." The moral is that no tool will tell one what one needs to check or reconcile, and this is not likely to change in the near future. Domain expertise is required and, as previously discussed, should be an important consideration in staffing the audit department.

Other important issues are obtaining the data and sampling. It is often said that sampling may be a thing of the past because with modern equipment one should be able to audit all data, not just a sample, which can be important if one is looking for relatively rare events. This may be true, but only if such planning has been made beforehand. It must be noted that not only has equipment advanced but also the data volume has increased. Many audit departments still lack the infrastructure to process all data. Furthermore, especially in today's fast-paced business environment, documentation may be of questionable quality or nonexistent, and the availability of personnel to explain the structure of data in, say, a data warehouse should not be taken for granted. Nor are administrators generally open to giving direct access to data on their machines to anyone, including auditors. These issues must be planned for, and it definitely should not be assumed that some miracle tool will correctly understand the data warehouse structure with no documentation or guidance.

Agility

Agility has to do with things that were always desirable,[10] such as more timely audits that focus on important aspects rather than "drive-by" audits.[11,12] There was never a real obstacle to implementing Agile audit other than the mind-set of some people at the top, plus the fact that Agile was not as popular at the time as it is now. The main driver for Agile being popular now is the accelerating pace of business, with significant changes happening in short time frames and large volumes. Often managers talk about agility as a buzzword, but few actually understand what this means. Even worse, the misconception arises that with being agile, one can adapt as one sees fit on all aspects. This could not be more untrue. First, there is no agility in contracts or other legal aspects. Agreements are not made to be changed unilaterally as one party sees fit. Second, agility does not mean doing away with planning or preparation; nor does it mean doing more with less, particularly less competent or less involved people. Agility is about being able to adapt to changing or unforeseen conditions, such as risk that emerges during fieldwork, but not necessarily during an initial walk-through or interviews.

That said, it is true that not only new technologies but also new trends put pressure on audit to change. For instance, DevOps challenges the concept of the traditional segregation of duties (SoD). Agile teams are less control-oriented; hence, there is even a philosophical difference. However, this does not mean that agility is an impediment in establishing needed controls. The controls must be based on need rather than custom or ritual. Indeed, if the developer wishes to add a time bomb to the code, how much assurance does SoD provide? On the contrary, nonrepudiation may be better served with DevOps, as there is in effect a one-stop-shop situation where a single party is responsible, in addition to less red tape and faster response. Should the auditor insist on SoD? No, it simply means that the auditor should identify important risk scenarios and propose measures commensurate with the organization's risk appetite to mitigate them. Such measures could involve strong detective controls such as logging and strong corrective controls—for example, rollback

> AGILITY DOES NOT MEAN DOING AWAY WITH PLANNING OR PREPARATION; NOR DOES IT MEAN DOING MORE WITH LESS, PARTICULARLY LESS COMPETENT OR LESS INVOLVED PEOPLE.

capabilities including stakeholders in the DevOps team to approve commits and process optimization and automation to minimize the number of people involved in nonautomated work. They could even involve extreme programming[13] (XP; pair programming), which is an Agile method calling for, among other things, programmers to work in pairs.

Many of these trends focus on efficiency and cost cutting. This is not new, but, as in the past, one is often reminded of the serious consequences of abolishing controls in the name of efficiency after the fact, typically when the next scandal hits the news, new legislation is passed and controls come back with a vengeance, much tighter than before.

Agility is not about replacing existing red tape with new Agile red tape. One does not need to use Scrum or Kanban. Agile is simply about asking, "How can a task be made more effective and efficient," especially in view of the fact that one typically does not have the full picture at the start of the audit? In the context of audit, it is about going back to basics and asking what are the main risk factors, how should they be evaluated and how should they be dealt with in an effective and efficient manner?

It is interesting that on some occasions, the people at the top (e.g., chief audit executive or equivalent) have jumped on the hype bandwagon of data analytics and agility without really understanding what these terms mean. Often those very same people are the ones who have established a formal and completely non-Agile audit environment that seriously impacts efficiency and effectiveness. A recent study found that "the biggest obstacle in the implementation is a missing mind-set in the sense of the basic mental attitude and attitude of the auditors and managers."[14] Similarly, some of these new advocates of data analytics, often with little if any field experience, would be hard-pressed to answer the question "What do you want to do with data analytics?" Their most likely answer would be to "lower costs," which misses the point entirely because a) the main point of analytics is to achieve more comprehensive results and b) the purpose of audit is to cover risk that is much more important than the audit costs. Needless to say, doing anything while being led by people who do not understand why this is being done offers little hope of success.

There is nothing preventing audit departments from becoming more agile by tailoring their audits to the situation in the field without having to follow strict protocol. For instance, there is little point in being Agile for a compliance audit, and there is no point in considering that obtaining and analyzing data prior to a finalized formal "audit program" is taboo, especially for new areas and systems with emerging risk. The only question is whether the audit leadership is ready for surrendering some control to the audit teams.

Conclusion

Although technological advances create both challenges and opportunities for the future of audit, audit fundamentals have not changed. They include the following:

- The audit function remains distinct from operations.
- Automated tools can help, but they are not a replacement for judgment.
- Asking the right questions is much more important than seeking a magic tool.
- Competence was always important and is not becoming any less important.
- Leadership and competence of the leadership team is important, and leadership needs to understand why something must be done instead of simply following the trends.

- Agility is essential and should be applied where it makes sense and where there is a gain to be made.
- Agility is not expensive to implement, but it takes leadership with effectiveness and efficiency credentials instead of a compliance and control mind-set.
- Agility does not mean replacing traditional audit with any specific framework.

> ALTHOUGH TECHNOLOGICAL ADVANCES CREATE BOTH CHALLENGES AND OPPORTUNITIES FOR THE FUTURE OF AUDIT, AUDIT FUNDAMENTALS HAVE NOT CHANGED.

Endnotes

1 Silver, D.; T. Hubert; J. Schrittwieser; I. Antonoglou; M. Lai; A. Guez; M. Lanctot; L. Sifre; D. Kumaran; T. Graepel; T. Lillicrap; K. Simonyan; D. Hassabis; "Mastering Chess and Shogi by Self-Play With a General Reinforcement Learning Algorithm," 5 December 2017, *https://arxiv.org/pdf/1712.01815*

2 Silver, D.; J. Simonyan; K. Antonoglou; I. Huang; A. Guez; A. Hubert; T. Baker; L. Lai; M. Bolton; A. Chen; Y. Lillicrap; T. Hui; F. Sifre; L. G. Van Den Driessche; T. Graepel; D. Hassabis; "Mastering the Game of Go Without Human Knowledge," *Nature*, vol. 550, 19 October 2017, *https://www.nature.com/articles/nature24270*

3 Alexiou, S.; "Advanced Data Analytics for IT Auditors," *ISACA® Journal*, vol. 6, 2016, *https://www.isaca.org/ archives*

4 Cangemi, M.; "Internal Audit's Role in Continuous Monitoring," *EDP Audit, Control, and Security Newsletter*, vol. 41, no. 4, April 2010

5 Kuhn, R. J.; S. Sutton; "Learning From WorldCom: Implications for Fraud Detection Through Continuous Assurance," *Journal of Emerging Technologies in Accounting*, vol. 3, no. 1, 2006

6 For management-perpetrated fraud, it is questionable whether any system that is ultimately under management control can be counted on to effectively detect or prevent the fraud.

7 Stelnick, R.; "Mainframe: Madoff-Size Money, Monstrous Misapplication—LOOP," 5 November 2011, *https://www.decodedscience.org/mainframe-madoff-size-money-monstrous-misapplication-loop/4927*

8 Byrnes, E. P.; A. Al-Awadhi; B. Gullvist; H. Brown-Liburd; R. Teeter; J. D. Warren; M. Vasarhelyi; *Evolution of Auditing: From the Traditional Approach to the Future Audit*, American Institute of Certified Public Accountants, USA, 2012, *https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/whitepaper_evolution-of-auditing.pdf*

9 Kaufman, F.; *Electronic Data Processing and Auditing*, Ronald Press Company, USA, 1961

10 Alexiou, S.; "Agile Audit," *ISACA Journal*, vol. 2, 2017, *https://www.isaca.org/archives*

11 Chambers, R.; "Drive-By Auditing: Don't Be Guilty of 'Hit and Run,'" *Internal Auditor*, 2 August 2012, *https://iaonline.theiia.org/drive-by-auditing-dont-be-guilty-of-hit-and-run*

12 Berkowitz, A.; R. Rampell; "Drive-By Audits Have Become Too Common and Too Dangerous," *The Wall Street Journal*, 9 August 2002, *www.wsj.com/articles/SB1028822538710052160*

13 Agile Alliance; "Extreme Programming," *https://www.agilealliance.org/glossary/xp/*

14 Botzenhardt, A. H.; T. Schommer; "Agile Auditing: Die Lösung der Revision für steigende Anforderungen—Empirische Studie zu Akzeptanzfaktoren und Hindernissen bei der Implementierung in nationalen und internationalen Innenrevisionen" ("Results Report: Agile Audit—Empirical study on Acceptance Factors and Impediments to Implementation in National and International Units"), *Zeitschrift für Interne Revision*, Ausgabe, Fachhochschule der Wirtschaft, 2019

Enjoying this article?

- **Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums***