Enhancing Audit Efficiencies: Maximizing the Use of Technology

By Karen Titus, KnowledgeLeader contributing writer

To help internal audit departments assess their options for enhancing audit efficiencies, a panel of experts convened for the September 2007, IIA webcast, "Enhancing Auditing Efficiencies: Maximizing the Use of Technology." In follow-up interviews with KnowledgeLeader, several of the participants – including Paul Sobel, who moderated the event - shared their views on the topic and discussed their own experiences and key areas related to maximizing technology use. This article is a two part series.

Ignore at your own peril

How important is technology to the audit process? Paul Sobel, vice president of internal audit, Mirant Corp., Atlanta, puts it bluntly: "If we ignore it, internal audit runs the risk of becoming irrelevant." That is certainly not a risk any internal auditor wants to take. Sobel believes that technology has inserted itself into nearly every aspect of contemporary organizations. He thinks internal audit (IA) could find itself behind the eight ball if it sticks with approaches used in the past. "I do not think traditional auditing – ignoring technology, auditing around the computer, not using the tools available to make an audit test more efficient or more effective - will cut it in the profession much longer," says Sobel.

Tim Grace, principal consultant of Tim Grace LLC, St. Louis, agrees that paying attention to technology is essential. "Technology represents up to 70 percent of the controls that should be in place," he points out. "So technology has to be there, and you have to audit technology."

John Verver, vice president of alliances and product strategy, ACL Services Ltd., Vancouver, British Columbia adds, "I think it will prove increasingly difficult to address their primary responsibilities in an effective way. When you look at the key risks relating to control and compliance, many of them now relate to technology. It is now important for internal audit to use technology to address the organization's technology-related risk and control issues."

If IA chooses to avoid technology other players are ready to step in. Sobel has witnessed other departments within companies starting to leverage off the technology and perform types of monitoring once considered the purview of IA. "That is not necessarily bad," he says, suggesting that companies might benefit from having management process owners perform more control activities, including monitoring.

"Likewise," he says, "outside vendors are trying to sell products or knowledge to help companies perform continuous monitoring and the like. I think there is a lot of value in that, although there is more value if it is done inside the company."

Given the importance of technology, it only makes sense for IA and management to work together to incorporate technology into the audit process. Though this can entail many strategies, simple communication is a good place to start.

"Both sides (management and IA) share a common goal and need to recognize that the IT audit function fits into the larger context of the business itself by enabling the business, helping the business drive the controls, and making sure the controls are in place," says Grace.

"It is best for audit to be involved from day one with new projects - that means upfront involvement. On existing projects it means IA needs to be woven into the fabric of what is already happening," says Sobel.

"From my experience, it is up to audit to make sure that relationship is a good relationship," Grace says. "I have come into situations where IT definitely does not want to talk to audit, they do not want to have anything to do with audit, and it has been a very contentious history. So, as an auditor you have to build that practice and relationship with IT, with technology."

Getting the right people on board

Sobel emphasizes the need for IA and management's process or control owners to participate in this process. He also adds a third piece to the mix: information technology professionals, since many key tools require access to data. Sometimes the ERP system is part of the equation, which means auditors need to not only comply with corporate policies that IT may have set up, but also use that resource to understand how to access that data, as well as the implications of doing so.

"Long term, IA may want to help develop or run these queries or data analysis applications before handing them off to management," says Sobel. "Have an upfront discussion: 'What are we trying to accomplish? Why? How are we going to do it? What are we going to do based on the results that we find?' This will create a more robust and targeted audit test and improve the likelihood of a smooth hand-off later on," states Sobel.

Verver sees an interconnected responsibility in continuous auditing and continuous monitoring. The general view in the profession is that the former is the responsibility of audit; the latter the responsibility of management. However, management is often reluctant to take a proactive approach to ongoing assessment and understanding control effectiveness.

The solution is often for audit to lead the way and provide the results of its continuous auditing processes to management. This provides practical evidence to management of the real value of taking a more proactive approach to controls assessment and helps management recognize that effective controls are good for business. "In the end, it usually makes sense for audit and management to work together on the ongoing assessment of the effectiveness of controls".

The current climate

It should surprise no one that technology has gained more attention of late. Once again, Sarbanes-Oxley (SOX) has been part of the push. Since testing controls can be fairly inefficient, continuous monitoring and continuous auditing techniques offer a welcomed improvement in terms of efficiency. "A lot of companies have been looking to do that, because it will reduce the overall SOX costs that were incurred early on," Sobel says.

Verver agrees that SOX has helped pique the interest of companies, especially as they look for ways to create an efficient and sustainable process. "It is not acceptable just to throw an awful lot of resources at the issue. This has to be a more thoughtful and automated and efficient process, and technology is the key to that," says Verver.

"There has been the recent focus on fraud prevention and detection, as companies try to spot fraud indicators that might otherwise bypass or fly under the radar of controls. Technology can be an important tool for identifying such anomalies and allows auditors to follow up on items that might not turn up in a more traditional controls-testing approach," Sobel says.

"Another influence," says Sobel, "is the prevalence of desktop applications. One of the interesting things that came out of SOX was the realization of how many spreadsheets are used in processing and how many actually support booking of financial entries or other key controls. Auditors have to be thinking differently about how to audit spreadsheets. That has also created more of a need for auditors to explore technology-based approaches when they are doing their internal audit projects."

Grace cites concerns about data leakage, "With the advent of mass storage devices, people can come in, plug these devices into the network easily – because you have USB ports on most computers nowadays – download data from the network, and just walk out the door."

"When technology is used efficiently, IA also experiences benefits to their risk management efforts. It can help detect risk events in a more timely way," says Sobel, "and perhaps allow for quicker, more comprehensive actions and reactions to risk events."

In addition, Sobel sees an improved ability to look at what he calls risk signposts – risk indicators that do not represent the actual occurrence of a risk, but do provide indications of a likelihood that the risk is now more likely to occur. As with more traditional risk detection, this will be heavily technology-focused, he predicts.

"Finally," says Verver, "continuous activities – of auditing, controls assessment, and monitoring – means an ongoing, far more efficient, automated process to determine that controls are working effectively, that key risks are in fact well-managed and that problem events and transactions are identified on a timely basis."

Finding a starting point

If a company is just beginning to consider how technology can benefit the audit process, how and where does it begin? Sobel suggests a three-pronged approach. "Research, research, research," he says. "KnowledgeLeader has some good places to start. Talk to other practitioners, and vendors are typically are ready and willing to share demos."

Sobel is also a big supporter of education. "Take a course for a few days on ACL, for example, because then you can devote yourself to the subject-matter. While you are there, you can immerse yourself and start thinking, 'OK, how can I use this at my company?'"

"If you start researching now," Sobel says, "maybe you can better figure out where technology makes the most sense in your company and in your audit department."

Grace begins with a basic question, "'How does technology affect the financial statements?' You go from there. However, that has to be in place before you can start looking at all the peripheral services that technology offers."

Good technology that supports audit management is part of the foundation as well, followed by technology to support audit and control testing processes, based on data analysis software. "We have seen over the last few years a very broad acceptance that audit analysis technologies and continuous auditing technologies, which are just a part of audit analysis overall, are key to the effective audit process," says Verver. "For a new audit department or audit department wanting to effectively include technology, it is really best to revisit the whole audit approach and audit strategy to make sure it can identify all the areas in which technology has a key role to play."

A shifting landscape

Sobel has seen a transformation in the way technology has been used in the IA process over the last decade or so. He cites two key changes: "It is now easier to use and much more powerful than in the early days. It is also readily available on a desktop, so almost any auditor with some – but not necessarily much – training can use technology, making it easier to build into the audit process. Audit technology is not the domain of IT auditors anymore; virtually any auditor can have that power – and this is a good power to have," admits Sobel. He sees several benefits from upping the use of technology in the audit process, including boosting efficiency and comprehensiveness.

A more subtle benefit is that it allows auditors to create new ways of testing information. He cites "ghosts" on the payroll as an example. "With technology, you can match an employee database with Social Security numbers against a national database of Social Security numbers – before you could not do that in an audit."

Sobel cautions that adding technology to the audit process can create its own set of challenges. "The biggest obstacle is creativity," he says. Now that auditors have easy access to technology, they need to ask, 'What are we going to do with this data? How can we use the data in such a way that it supplements the audit process?'"

All too often, Sobel says, "Auditors tend to think of technology as a tool to automate what they were already doing, albeit with 100 percent of the population rather than the sample. That is not bad, but it is not creative. To overcome such inertia, organizations would be wise to have a handful of department members create a list of all available data fields, then step back and say, 'What else can we do?' Sometimes that will unleash ideas that individuals may not have thought of on their own."

Based on his own experience, Sobel notes that open minds can be a tremendous asset in effective technology use. While younger employees may be quite comfortable with technology, they lack the business experience and acumen of older employees. In the best-case scenario, organizations will marry the comfort and knowledge around technology with the business knowledge. "For me, when we are starting an audit, I will say, 'How can we use technology here?' And I will actually push on people to figure out how we can better use technology," he says.

Data analytics

Technology has a strong presence in the area of data analytics, which, in turn, has a key role in the IA process. "Data analytics allows auditors to independently have insight into business process systems and financial transactions and control systems that they are responsible for auditing," says Verver. Data analytics got its start some 20 years ago. "At that time, it was very much a role for specialists and for performing fairly limited activities," Verver says. The Big Eight/Big Six firms developed their own software for computer-assisted audit technique – as it was then called – to do tasks such as statistical sampling.

"There has been a tremendous evolution since then," he continues. The technology is now used throughout audit teams, rather than being confined to specialists; moreover, the analyses have become quite sophisticated, testing 100 percent of transactions, for example, to look for specific instances or indications of fraud, error, operational inefficiencies, and so on.

The training needed to use this technology for the typical non-technical auditor, is hardly overwhelming. Verver estimates it at three days, followed by online training for just-in-time-assistance. "It is relatively short, but in most internal audit departments, the effective use of data analysis requires a model where there is also a specialist resource available to deal with the more complex issues that might arise. So, that technical background would require substantially more training."

Verver believes in order to be truly effective, especially in larger organizations with sizeable IA departments, an IT specialist – perhaps an IT auditor – should be involved from the get-go. “It is essential that someone knowledgeable work with the IT department to arrange data access and downloading, then deal with issues of data structures and storage, provide assurance over security of the data, and deal with some of the technical issues. This specialist role is important for enabling less technical auditors to maximize the benefits that can be achieved from analytics software.” Verver also notes that it is important that an appropriate individual be given the role of reviewing the procedures performed by auditors to ensure they are logically correct and that good control has been maintained throughout the data analysis process.

Organizations can incorporate data analytics into the audit process in several ways. One good place to start is to go through an audit program at the audit planning stage and identify the stages in which data analytics can be most usefully applied. “That is a common approach,” Verver says.

Once data analytics is incorporated into the audit, what process improvements might companies expect to identify? “There is a lot of evidence that the use of data analytics achieves a number of things. One is typically a substantial reduction in time required for substantive testing and for testing of the controls,” Verver says. A second benefit is increased assurance. “Rather than just testing a judgmental or a statistical sample, you are able to test 100 percent of the population and obtain a high rate of confidence as a result.”

“Indeed,” he adds, “audit departments frequently are able to identify error, fraud or other problems and quantify the amount – adding another, bottom-line benefit if the dollars can be recovered or the control improved.”

The real issue, Verver says, is that despite the growing awareness in recent years of the role of data analytics, many IA departments nevertheless fail to understand that it must be an integral part of the audit process. Like any other part of the audit process, the use of data analytics should be properly planned, managed and controlled. Although a certain level of technical expertise is important within the process, its use should not be confined to specialists and expertise should not be locked up in silos but made available to an audit team in a collaborative environment.

Continuous monitoring

Continuous monitoring is an idea whose time has come. “Actually, it is long overdue,” says Grace. “We, in internal audit, have been talking about continuous monitoring for a long time,” he says, “but it has never quite gotten to where it should be within the audit world.” SOX, however, has begun to change the picture.

“Continuous monitoring ensures there are procedures and processes in place to continuously monitor controls that should be in place. “The best thing I can point to is identity and access management systems, because you are reviewing, on a minute-by-minute, second-by-second basis who has access to your system and what types of accesses they have – and what they are actually accessing,” Grace explains. “Going forward, monitoring such activity logs will be key to the entire monitoring process and its development,” he predicts.

“As in other technology-based endeavors, the use of continuous monitoring requires few specialized IT skills,” Grace says. Current vendor products are quite self-explanatory and do not require the skills of a hands-on developer with deep technical knowledge, as older systems did. “They are getting a lot easier.”

“The bigger challenge may be to make sure management and internal audit fulfill their roles. Management needs to be the driving force behind any continuous monitoring efforts,” says Grace. Likewise, it is up to internal audit to pick up the ball and reinforce the process. “They are the ones who hold management responsible for what is going on.”

Grace offers a final thought regarding the roles of these two groups: “They are both working toward one common goal, and that is to make sure effective controls are in place within the organization.”

Article from Protiviti KnowledgeLeader – www.knowledgeleader.com.

KnowledgeLeader is a subscription-based website that provides audit programs, checklists, tools, resources and best practices to help internal auditors and risk management professionals save time, manage risk, and add value. Free 30-day trials available.

Protiviti is a leading provider of truly independent internal audit and business and technology risk consulting services. We help clients identify, measure and manage operational and technology-related risks they face within their industries and throughout their systems and processes. And we offer a full spectrum of audit services, technologies and skills for business risk management and the continual transformation of internal audit functions.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.