Six Steps to an Effective Continuous Audit Process

Establishing priority areas and determining the process' frequency are two of the six steps that internal auditors and senior managers need to take into consideration before making the switch to continuous auditing.

Carlos Elder de Aquino
Chief Auditor, Unibanco

Washington Lopes da Silva
IT Audit Superintendent, Unibanco

Nilton Sigolo
Manager, Continuous Auditing, Unibanco

Miklos A. Vasarhelyi
Professor of Accounting, Business Ethics and Information Systems, Rutgers University

The need to improve and accelerate audit activities has led in part to the increased adoption of continuous auditing as a vital monitoring tool. Initially recorded at AT&T Corp. by its Bell Laboratories research center during the late 1980s and early 1990s, continuous audit efforts are now under way in organizations including Siemens, HCA Inc., Unibanco, the New York Federal Reserve, and IBM. Additionally, legislation such as Section 404 of the U.S. Sarbanes-Oxley Act of 2002 and audit software vendors, including ACL, IDEA, Approva, and Oversight, are molding and giving large momentum to the continuous audit field. Consequently, as continuous auditing continues to grow around the world, internal auditors and senior managers need to understand the necessary actions required to support an effective continuous audit process, including establishing audit priority areas and determining the process' frequency.

BEFORE PITCHING THE IDEA

When organizations begin evaluating the adoption of continuous auditing, three common issues usually arise that if expected can be managed effectively. First, is the confusion among auditors and senior management regarding the differences between continuous auditing and continuous monitoring. Second, is the need for auditors to understand the role of continuous auditing as a meta control (i.e., a control of controls). And third, is the concern that implementing continuous auditing will lead to a loss of independence and objectivity as audit professionals become operationally involved in the process. While the way in which companies address these challenges will be unique to their organization, the following best practices can help them prepare for these issues.

What is Continuous Auditing?

According to The Insitute of Internal Auditors' (The IIA) Global Technology Audit Guide (GTAG) *Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*, continuous auditing is defined as the automatic method used to perform control and risk assessments on a more frequent basis. As the guide states, technology plays a key role in continuous audit activities by helping to automate the identification of exceptions or anomalies, analyze patterns within the digits of key numeric fields, review trends, and test controls, among other activities. Other organizations, such as the American Insitute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (AICPA/CICA) have further defined continuous auditing and provided guidance on the subject.

For additional basic information on continuous auditing, read *ITAudit's* "Recommendations for an Effective Continuous Audit Process" and "Making the Change to Continuous Auditing." To learn how to implement a continuous online audit system, read "Continuous Online Auditing in the Government Sector," which is also available on *ITAudit*.

To learn more about how you can view the entire broadcast, visit The IIA's webcast offerings.

Continuous Monitoring Vs. Continuous Auditing

Typically, continuous monitoring is a management function to ensure that company policies, procedures, and business processes are operating effectively and addresses management's responsibility to assess the adequacy and effectiveness of internal controls. In addition, continuous monitoring usually involves the automated testing of all transactions and system activities within a given business process area against control rules. Monitoring may occur on a daily, weekly, or monthly basis based on the nature of the underlying business cycle.

Although many of the continuous monitoring techniques used by management are similar to those performed by internal auditors during continuous audit activities, continuous auditing usually enables auditors to evaluate the adequacy of management's monitoring function and identify and assess risk areas. In addition, clearly communicating the differences between the two will aid in avoiding confusion or resistance to continuous auditing as a redundant effort. (For more information about the differences between continuous monitoring and continuous auditing, please refer to The IIA's GTAG on continuous auditing.)

Meta Control

Continuous auditing also tends to be dynamic in nature (i.e., the auditor can turn continuous audit processes on and off based on current system loads by reconfiguring these activities according to the internal audit plan). Therefore, by monitoring particular configurable items, continuous auditing provides an additional level of controls and acts as a metal control.

For example, a bank can issue an alarm under pre-specified circumstances to the bank manager's supervisor whenever loans reach a pre-authorized level. This activity then increases the level of controls that can be configured, such as by including the choice to have an alarm issued and under which circumstances.

Figure 1. Illustration of the continuous audit process' dynamic nature

Independence and Objectivity

Finally, because continuous audit activities are different from those taking place during a more traditional audit, audit principles need to be re-conceptualized. This is because continuous auditing often places the auditor in the middle of the transaction flow. For instance, at a major US-based electronic brokerage firm that monitors its client's electronic transactions, auditors are notified when a transaction is blocked after certain analytical parameters are met. The auditor then deals directly with the client. As this example illustrates, it is important for internal auditors to make sure that the continuous audit process has a system of checks and balances to maintain the independence and objectivity of their work throughout the audit.

KEY STEPS TO IMPLEMENTING CONTINUOUS AUDITING

Once the issues above are understood by managers and auditors alike, the organization will be in a better position to begin using continuous auditing. Generally, the implementation of continuous auditing consists of six procedural steps, which are usually administered by a continuous audit manager. Knowing about these steps will enable auditors to better monitor the continuous audit process and provide recommendations for its improvement, if needed. These steps include:

1. Establishing priority areas.
2. Identifying monitoring and continuous audit rules.
3. Determining the process' frequency.
4. Configuring continuous audit parameters.
5. Following up.
6. Communicating results.

Below is a description of each.

Figure 2. Continuous audit implementation steps

1. Establishing Priority Areas

The activity of choosing which organizational areas to audit should be integrated as part of the internal audit annual plan and the company's risk management program. Many internal audit departments also integrate and coordinate with other compliance plans and activities, if applicable. (Steps 2-6 below are applicable to all of the priority areas and processes being monitoring as part of the continuous audit program.)

Typically, when deciding priority areas to continuously audit, internal auditors and managers should:

> Identify the critical business processes that need to be audited by breaking down and rating risk areas. Understand the availability of continuous audit data for those risk areas. Evaluate the costs and benefits of implementing a continuous audit process for a particular risk area. Consider the corporate ramifications of continuously auditing the particular area or function. Choose early applications to audit where rapid demonstration of results might be of great value to the organization. Long extended efforts tend to decrease support for continuous auditing. Once a demonstration project is successfully completed, negotiate with different auditees and internal audit areas, if needed, so that a longer term implementation plan is implemented.

When performing the actions listed above, auditors need to consider the key objectives from each audit procedure. Objectives can be classified as one of four types: detective, deterrent (also known as preventive), financial, and compliance. A particular audit priority area may satisfy any one of these four objectives. For instance, it is not uncommon for an audit procedure that is put in place for preventive purposes to be reconfigured as a detective control once the audited activity's incidence of compliance failure decreases.

2. Monitoring and Continuous Audit Rules

The second step consists of determining the rules or analytics that will guide the continuous audit activity, which need to be programmed, repeated frequently, and reconfigured when needed. For example, banks can monitor all checking accounts nightly by extracting files that meet the criterion of having a debt balance that is 20 percent larger than the loan threshold and in which the balance is more than US $1,000.

In addition, monitoring and audit rules must take into consideration legal and environmental issues, as well as the objectives of the particular process. For instance, how quickly a management response is provided once an activity is flagged may depend on the speed of the clearance process (i.e., the environment) while the activity's overall monitoring approach may depend on the enforceability of legal actions and existing compliance requirements.

3. Determining the Process' Frequency

Although the process is called continuous auditing, the word continuous is in the eye of the beholder. Auditors need to consider the natural rhythm of the process being audited, including the timing of computer and business processes as well as the timing and availability of auditors trained or with experience in continuous auditing. For instance, although increased testing frequency has substantial benefits, extracting, processing, and following up on testing results might increase the costs of the continuous audit activity. Therefore, the cost-benefit ratio of continuously auditing a particular area must be considered prior to its monitoring.

Furthermore, other tools used by the manager of the continuous audit function include an audit control panel in which frequency and parameter variations can be activated. Hence, the nature of other continuous audit objectives, such as deterrence or prevention, may determine their frequency and variation.

4. Configuring Continuous Audit Parameters

Rules used in each audit area need to be configured before the continuous audit procedure (CAP) is implemented. In addition, the frequency of each parameter might need to be changed after its initial setup based on changes stemming from the activity being audited. Hence, rules, initial parameters, and the activity's frequency also a special type of parameter should be defined before the continuous audit process begins and reconfigured based on the activity's monitoring results.

When defining a CAP, auditors should consider the cost benefits of error detection and audit and management follow-up activities. For instance, in the example of the bank described earlier, the excess threshold of US $1,000 could lead to a number of false negatives (e.g., values that were ignored when the balance was smaller than US $1,000 but were identified as representing a problem) and a number of false positives (e.g., values with balances above US $1,000 that were flagged but were accurate). If the threshold is increased to US $2,000, there will be an increase in false negatives and a decrease in false positives. Because follow up costs would go up as the number of false positives increases and the presence of false negatives may lead to high operational costs for the organization, internal auditors should regularly reevaluate if error detection and follow-up activities need to be continued, reconfigured, temporarily halted, or used on an ad hoc basis.

Furthermore, the stratification of audited data into sub-groups allows organizations to better monitor the activity and reconfigure any parameters (e.g., auditors will be notified when balances larger than 20 percent of the debt remain that are also larger than US $5,000). However, the more complex the rule and its conditional components, the more parameters that must be examined, monitored, and sometimes reconfigured.

5. Following Up

Another type of parameter relates to the treatment of alarms and detected errors. Questions such as who will receive the alarm (e.g., line managers, internal auditors, or both usually the alarm is sent to the process manager, the manager's immediate supervisor, or the auditor in charge of that CAP) and when the follow-up activity must be completed, need to be addressed when establishing the continuous audit process.

Additional follow-up procedures that should be performed as part of the continuous audit activity include reconciling the alarm prior to following up by looking at alternate sources of data and waiting for similar alarms to occur before following up or performing established escalation guidelines. For instance, the person receiving the alarm might wait to follow up on the issue if the alarm is purely educational (i.e., the alarm verifies compliance but has no adverse economic implications), there are no resources available for evaluation, or the area identified is a low benefit area that is mainly targeted for deterrence.

6. Communicating Results

A final item to be considered is how to communicate with auditees. When informing auditees of continuous audit activity results, it is important for the exchange to be independent and consistent. For instance, if multiple system alarms are issued and distributed to several auditees, it is crucial that steps 1-5 take place prior to the communication exchange and that detailed guidelines for individual factor considerations exist. In addition, the development and implementation of communication guidelines and follow-up procedures must consider the risk of collusion. Much of the work on fraud indicates that the majority of fraud is collusive and can be performed by an internal or external party. For example, in the case of dormant accounts, both the clerk that moves money and the manager that receives the follow-up money may be in collusion since the manager's key may have to be used for certain transactions.

ADDITIONAL CONSIDERATIONS

Besides the six steps described in the previous section, two additional issues that emerge when implementing continuous auditing are the infrastructure needed for the process to work and its impact on the workplace.

Organizational Infrastructure

Because continuous auditing is a part of the company's audit function, it must be kept independent of management. Therefore, during the planning stages, auditors need to keep in mind the process' independence when designing its structure. For instance, a typical internal audit department is structured so that areas of the department focus on different cycles or business activities. In addition, the department may be divided into financial and IT audit functions.

Sometimes, however, IT audit activities are incorporated as part of existing IT operations. In organizations such as these, the development of continuous auditing is usually delayed because the activity may not get the necessary development priority. Regardless of whether IT audit activities are part of the organization's IT or internal audit department, the organization must maintain the process' independence as well as allocate resources in support of continuous audit activities.

Impact on Personnel

In addition, the audit manager in charge of the continuous audit process should have a more technical understanding of IT as well as extensive experience on the activities being audited. However, hiring, training, and retaining auditors who can implement and monitor continuous audit activities might be challenging due to the scarcity of internal auditors with knowledge in the area. Furthermore, the continuous audit process might create a daily stream of issues that need to be resolved, which might prove stressful given current personnel resources, and might require the continuous audit manager to exert adequate authority in moments of exceptions.

FINAL THOUGHTS

While more organizations are progressively implementing continuous auditing and, along the way, improving the quality of the data gathered during each audit auditors and managers that are looking to implement a continuous audit approach need to be willing to move beyond their traditional yearly audit activities. Although not a lot of guidance exists today about the best ways to implement a continuous audit process, as with any major change, the evolution toward continuous auditing will take time and substantial attention from senior management.

Carlos Elder Maciel de Aquino is the chief auditor for Unibanco in Brazil. He has 26 years of experience in internal audit of financial institutions and has helped design and teaches at the MBA in Internal Audit program at FIPECAFI, the Institute Foundation of Financial, Accounting, and Actuarial Research in Brazil. Maciel de Aquino graduated in accounting from the Federal University of Pernambuco and holds post-graduate degrees in economics engineering and in business finance. Aquino also holds an executive master's degree in business administration (MBA) from the Brazilian Institute of Capital Markets and an MBA from the University of S梓Paulo.

Washington Lopes da Silva is head of IT audit at Unibanco in Brazil and has a master's degree in electrical engineering from the Mackenzie Presbyterian University in S梓Paulo, Brazil. He has 15 years of experience in IT, auditing, and consulting. Prior to Unibanco, he worked at Ernst & Young and KPMG and taught a course on electronic services and products at S梓Paulo's Bandeirante University. Lopes da Silva is also the chair of the IT Audit Committee of FEBRABAN, the Brazilian Bank Association.

Nilton Sigolo has worked for Unibanco for nearly four decades. He is currently an internal audit manager for the bank where manages the distance audit group that is responsible for Unibanco's continuous audit monitoring and control. He is a graduate of the Universida de Mackenzie with a major in computer sciences.

Miklos A. Vasarhelyi, Ph.D., is currently the KPMG professor of accounting information systems and director of the Continuous Auditing and Reporting Laboratory at Rutgers University. He is also the technology consultant at the AT&T Laboratories. He has published more than 110 journal articles and 18 books and has taught executive programs on electronic commerce to many large international organizations, including ADL, AT&T Corp., Baxter Healthcare, Chase Bank N.A., Eli Lilly and Company, GE, J&J, Siemens, and Volvo Cars. In addition, he is the editor of the Artificial Intelligence in Accounting and Auditing series and of two academic journals. Vasarhelyi got his doctorate degree in management information systems from the University of California, Los Angeles, and an MBA from the Massachusetts Institute of Technology.

Site Search:

The Institute of Internal Auditors - 247 Maitland Avenue Altamonte Springs, Florida 32701-4201 U.S.A.
+1-407-937-1100 Fax +1-407-937-1101 www.theiia.org

Home| About The IIA | About ITAudit | Privacy Policy