On the Road to Continuous Auditing

Carlos Elder de Aquino
Washington Lopes da Silva
Miklos A. Vasarhelyi

Establishing audit priority areas can lead to a more effective continuous audit process.

Initially conducted at AT&T Corp. by its Bell Laboratories research center during the late 1980s, continuous audit efforts are now under way in many leading 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 are molding and giving momentum to the continuous audit field. Consequently, as the use of continuous auditing increases around the world, internal auditors and senior managers need to understand the necessary steps to support an effective continuous audit process that meets the organization's audit objectives.

INITIAL CONSIDERATIONS

As organizations evaluate 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 managers 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.

Continuous Monitoring vs. Continuous Auditing

As a management function, continuous monitoring helps ensure company policies, procedures, and processes operate effectively and assesses the adequacy of internal controls. Continuous monitoring usually involves the automated testing of transactions and system activities within a given business process area against control rules and may occur on a daily, weekly, or monthly basis based on the nature of the underlying business cycle.

On the other hand, continuous auditing is the automated performance of control and risk assessments on an ongoing basis. According to the IIA's *Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*, 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.

Deleted: T

Although many continuous monitoring techniques are similar to those performed during continuous audit activities, continuous auditing 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 avoid confusion or resistance to continuous auditing as a redundant effort.

Meta Control

Continuous auditing tends to be dynamic in nature (i.e., the auditor can turn continuous audit processes on and off by reconfiguring activities according to the internal audit plan). Therefore, by monitoring particular configurable items, continuous auditing provides an additional level of controls acting as a metal control. For example, the bank's internal audit monitoring system 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 having the choice to issue an alarm and under which circumstances.

Deleted: a

Deleted: . **[If the alarm is going to bank management, then it looks like a CM activity. This statement may add to the confusion between what is or uses CA or CM. Please use a different example to avoid further confusion.]**

Independence and Objectivity

Internal audit principles may need to be reconceptualized before a continuous audit process is established. This is because continuous audit activities are different from those taking place during a more traditional audit, often placing the auditor in the middle of the transaction flow. For instance, at a major 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 objectivity of their work throughout the audit.

Comment [MAV1]: Independence is different under continuous audit… we aim at objectivity more than th ecurrrent pseudo independence.. just more like the Canadian standrds

Deleted: the independence and

Deleted: **[If I understood the example correctly, you are stating that an independent, internal auditor is placed in the middle of the transaction flow. Thus, he or she is part of operations, contacting the client and resolving issues. However, this does not sound like it achieves the audit independence principle. Please use another example or state that the auditor turns the issue over to another group, like security, for resolution.]**¶

KEY STEPS

After initial concerns are identified and managed, the organization should be ready to implement the continuous audit program. Generally, implementation of continuous auditing consists of six procedural steps usually administered by a continuous audit manager.

1. Establish 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. 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 risk areas.
- Evaluate the costs and benefits of continuously auditing a particular risk area.
- Consider the corporate ramifications of continuously auditing an 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 completed successfully, negotiate with different auditees and internal audit areas, so that a longer-term implementation plan is implemented.

In addition, 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 put in place for preventive purposes to be reconfigured as a detective control once the activity's incidence of compliance failure decreases.

2. Identify rules. The second step consists of determining the rules or analytics that will guide the continuous audit activity. These rules 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, audit rules must consider legal and environmental issues and 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. Determine the process' frequency. Auditors need to consider the natural rhythm of the audited process, including the timing of computer and business processes and 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. 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. An audit control panel is a dashboard to be used by the auditor to manage the continuous audit process. Hence, the nature of other continuous audit objectives, such as deterrence or prevention, may determine the process' frequency and variation.

Deleted: [Please define this term.]

4. Configure parameters. Rules used in each audit area need to be configured before the continuous audit procedure (CAP) is implemented. Additionally, the frequency of each continuous audit parameter may need to change after its initial setup based on modifications to the audited activity. Hence, rules, initial parameters, and the activity's frequency — also a special type of parameter — should be defined before the continuous audit process begins.

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 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 will go up as the number of false positives increases and the presence of false negatives may lead to high operational costs, auditors should reevaluate regularly if error detection and follow-up activities are continued, reconfigured, temporarily halted, or used on an ad hoc basis.

5. Follow 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.

Continuous monitoring is a basic feature of continuous audit. Anaytics used by management and audit for exception detecting may be different. Auditors may have alarms that are exclusive to auditing and others that may also be issued to different levels of management.

Deleted: [Why would CA reports go to line managers? Please rephrase to avoid the confusion between CA and CM. For instance, CA reports go to the auditor, while CM reports go to line managers.]

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

6. Communicating Results A final item to be considered is how to communicate with audit clients. When informing clients on 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 clients, it is crucial that steps 1–5 take place before the communication exchange and detailed guidelines for individual considerations exist. In addition, the development and implementation of communication guidelines and follow-up procedures must consider the risk of collusion. In the case of dormant accounts, for example, the clerk that moves money and the manager that receives the follow-up money may be in collusion as the manager's key needs to be used for certain transactions.

CONTINUOUS IMPROVEMENT

As more organizations continue to adopt continuous auditing — and, along the way, improve the quality of the data gathered during each audit — auditors looking to implement a continuous audit approach need to be willing to move beyond their traditional yearly audit activities. Although little guidance exists on the best ways to implement a continuous audit process, the evolution toward continuous auditing will take time, substantial attention from senior management, and the use of additional costs and resources as continuous audit activities are implemented and sustained.

Carlos Elder Maciel de Aquino is the chief auditor for Unibanco in São Paulo, Brazil.

Washington Lopes da Silva is head of IT audit at Unibanco.

Miklos A. Vasarhelyi, Ph.D., is the KPMG professor of accounting information systems and director of the Continuous Auditing and Reporting Laboratory at Rutgers University in Newark, N.J.

To comment on this article, e-mail the authors at miklos.vasarhelyi@theiia.org

Deleted: [We provide one of the authors with an internal e-mail address to receive feedback on the piece. If you prefer that Carlos or Washington have the e-mail address let me know. Also, the bios we edited by the editor-in-chief for space purposes.]