



Information Systems Control Journal, Volume 5, 2002

Continuous Auditing: Is It Fantasy or Reality?

By ISACA Standards Board

The concept of continuous auditing has been around for many years. It has been talked about, researched and theorized. Many organizations have made significant investments of time and money, yet for most organizations it is nothing more than an unrealized dream. As a matter of fact, one organization's version of continuous auditing may differ dramatically from another organization's implementation. Why is that? Why are organizations or auditors unable to breach the gap and turn this concept into reality? Why is there not even a consensus definition of continuous auditing?

What Is Continuous Auditing?

Continuous auditing has been defined as a methodology or framework that enables auditors (external and internal) to provide written results on the subject matter using one or a series of reports issued simultaneously. The ability to report on events in a real-time or near real-time environment can provide significant benefits to the users of audit reports. Continuous auditing is therefore designed to enable auditors to report on subject matter within a much shorter timeframe than under the traditional model. Theoretically, in some environments it should be possible to decrease the reporting timeframe to provide almost instantaneous auditing.

In the traditional audit model used by internal and external auditors, a period of time passes between the completion of fieldwork and issuance of the audit report. In many instances, the impact of this delay makes the information contained in the report less useful or beneficial to the user. This is caused by the historical nature of the information contained in the report, which can be affected by such issues as auditee corrections to identified deficiencies, and deterioration in the control environment (or related auditee data) resulting from identified control weakness or from significant subsequent events that materially affect the original audit opinion.

In the external audit world, the ability to provide audit level auditing on real-time financial information could have a significant impact on an organization's market capitalization and on its cost of capital. In fact, Harvey Pitt, chairman of the US Securities and Exchange Commission, said in a recent speech that "[we] need to move toward a dynamic model of current disclosure of unquestionably material information." It is certain there is tremendous need for current disclosure of financial information. Furthermore, there is no doubt that the value of that information, when accompanied by an external audit opinion, will be enhanced.

In the internal audit world, the ability to provide management with real-time auditing on the functioning of controls and on financial transactions can enhance significantly management's ability to make key business decisions.

What Is Continuous Monitoring?

Continuous monitoring allows an organization to observe the performance of one or many processes, systems or types of data. In many respects, continuous monitoring systems are similar to executive information systems. Executive information systems are designed to provide users with summary information about an organization's transactions, such as daily sales volume, orders received and shipments. Continuous monitoring systems provide similar information on processes, systems and data. For example, one large telecommunication company has made significant investments in continuous monitoring systems designed to monitor daily transaction volume. These systems identify fluctuations in call volume and help ensure all placed calls are billed. In fact, they even identify possible situations where call fraud, such as a stolen calling card, is occurring. Other organizations have developed continuous monitoring systems that monitor accounts payable and cash disbursement activity. These systems are designed to look for double payments by comparing invoice numbers, vendor numbers and payment amounts to paid invoice files.

Is Continuous Monitoring the Same as Continuous Auditing?

No. The end result of continuous monitoring is to obtain information about the performance of a process, system or data, not the issuance of an audit report. As a result, there are key differences.

The first difference is in the type and sufficiency of evidence generated by continuous monitoring systems. Attestation standards issued by the American Institute of Certified Public Accountants (AICPA) state that, "Sufficient evidence shall be obtained to provide a reasonable basis for the conclusion that is expressed in the report." (Many countries have standards with similar wording.) These attestation standards further state that evidence obtained from independent sources provides the highest level of proof as does evidence obtained from direct examination. Information obtained from an IS auditor's direct personal knowledge (such as through physical examination, observation, computation, operating tests or inspection) is more persuasive than information obtained indirectly. Information from a continuous monitoring system provides indirect information about the performance of a process, system or data, whereas information obtained through an IS auditor's observance of a process or system, reperformance of a control, or testing of data provides direct evidence about the process, system or data.

In a continuous auditing engagement, the IS auditor's objective is to accumulate sufficient evidence to reduce risk to a level that is, in the practitioner's professional judgment, appropriately low for the high level of auditing imparted by the report. This means that an IS auditor must select procedures that provide sufficient evidence about a particular subject matter. The type of procedures performed is based on the IS auditor's assessment of inherent, control and detection risk. The extent to which selected procedures are performed is based on factors such as materiality, risk of errors and likelihood of misstatements. Information provided by continuous monitoring systems can provide IS auditors with significant information about a process, system or data, but due to its indirect nature, that information alone would not be sufficient in a continuous auditing engagement.

The second issue with continuous monitoring systems is more fundamental. The monitoring of processes and systems is a management function. AICPA audit standards state, in part, "Management monitors controls to consider whether they are operating as intended." This clearly indicates that the monitoring of processes, systems and data is a management control function. When an IS auditor performs a management control function, independence is impaired. As a result, the use of continuous monitoring systems by IS auditors may create situations where the IS auditor's independence is impaired.

For example, consider an environment where management uses the monitoring system, evaluates its output, identifies error conditions and responds to those errors. If the IS auditor tests the use of the monitoring system by management, then independence should be preserved. However, if the IS auditor identifies the error condition and alerts management, then independence would be impaired. In that situation, the IS auditor performed the management control function, not management.

Is Continuous Auditing an Attainable Goal?

While there has been significant academic research on the subject, as well as multiple efforts by professional standard-setting bodies around the world, there has been little, if any, reporting on a continuous basis. This is a result of a number of factors, which include such things as demand, cost vs. benefit and technological issues.

While the concept of continuous auditing has been around for many years the actual practice and demand for this service has been low. At least from the external audit perspective, this is a result of the perceived cost outweighing the perceived benefit. This viewpoint is a direct result of looking at continuous auditing only from the financial reporting perspective. Unquestionably, the cost of issuing an audit report on a full set of financial statements each week, month or quarter would be significant and would exceed its value. However, if the audit report only addressed specific types of relevant financial or nonfinancial data, performance measures or some other information that was of value to users and could be audited at a reasonable cost, then the benefits of this type of reporting may exceed its cost. The important lesson is simple. If continuous auditing is to establish itself, organizations and IS auditors must start small. They should start with easily auditable data that has significant value to users, such as investors and the equity markets, and structure an engagement to allow an IS auditor to report in a timeframe that provides value to users of data.

Many organizations are not ready for continuous auditing from either a maturity level or a technological level. This is a factor of the maturity of their processes, systems and controls. The cost and time needed to perform a continuous auditing engagement increases as the strength of an organization's processes and controls decreases. Organizations with strong processes and controls and mature systems are better suited to a continuous auditing engagement because the IS auditor can place greater reliance on the processes, controls and systems to reduce the extent, nature and timing of testing to support a continuous auditing opinion. For example, if an organization wanted to release audited monthly sales and production information two days after month end, the IS auditor must perform all audit procedures within two days (in most situations, this would not be practical) to meet the reporting deadline. Conversely, the IS auditor could place reliance on the processes and controls over the systems that process monthly sales and production data and test those processes, controls, systems and data over the month. This would better enable the IS auditor to meet the reporting deadline.

Another factor is technology. In the prior example, the IS auditor needs to collect data on monthly sales and production

activity as well as data on the functioning of processes and controls. This could be done at month-end or during the month. If the IS auditor chose to collect and analyze this information during the month, then he/she would need a method to accomplish this without disruption to the client's processing environment. With the widespread adoption of relational databases, increased sophistication of electronic audit tools and the proliferation of remote access through virtual private networks and secure socket layer technology, the ability of IS auditors to passively access client data has increased substantially. Internal and external IS auditors can access data stored in relational databases easily for analysis and testing while maintaining security over proprietary information.

What Does Continuous Auditing Mean to IS Auditors?

To report on a continuous basis, an organization must have strong controls. Many of these controls exist within and around IT systems. The special skills and knowledge that IS auditors have are essential to the assessment of these controls and to the performance of these engagements. This means that IS auditors are the key to the issuance of any continuous auditing report, regardless of its subject matter. This concept is supported by research done in a 1998 study jointly issued by the Canadian Institute of Chartered Accountants (CICA) and the AICPA. The research discussed many of the concepts and issues associated with continuous auditing. It looked at a variety of topics including what types of subject matter were suited to continuous auditing reporting and the types of control environments best suited for continuous auditing. The study concluded that organizations with strong internal control environments and well-controlled information systems were best suited for continuous auditing. This conclusion was based on the assumption that, to make continuous auditing possible and cost effective, significant reliance on controls was required. The study noted that IS auditors would have a significant involvement in continuous auditing engagements as it was expected that many of the controls would be IT controls.

In the internal audit environment, the concept is no different. If an internal auditor undertakes a continuous auditing engagement, the same concepts apply.

In the example where the IS auditor reports on monthly sales and production data, the report on information comes directly from the organization's information systems. As a result, the need to examine IT controls over systems that generate the monthly sales and production data is the key to being able to issue a report.

A real-life example can be found in the SysTrust service jointly developed by CICA and AICPA. SysTrust allows an IS auditor to report on the controls over a system. Depending upon the nature of the system under examination, the controls may be significantly, or entirely, comprised of IT controls. Many of the issued SysTrust opinions cover IT systems including systems hosted by third-party providers. In all of these reports, IS auditors have played a significant part in the performance of these engagements. An interesting aspect is that SysTrust engagements can be performed on a continuous basis and can be used to provide continuous auditing over a system.

Implementing Continuous Auditing

If an organization is considering implementing continuous auditing (whether performed by external or internal IS auditors), there are multiple issues to consider, including:

- Subject matter
- Environment
- Nature of testing required
- Timing

Unquestionably, the first step is to define appropriate subject matter. Attempting to perform a continuous auditing engagement on the entire set of financial statements for a multinational organization with disparate systems is virtually impossible. On the other hand, performing a continuous auditing engagement on daily production, shipments, sales or other tangible and easily quantifiable subjects is much easier. This includes the controls over many applications such as a loan processing system, credit-card processing system and B2B systems. The point is fairly straightforward: subject matter that is definable and measured easily is most conducive to continuous auditing. On the other hand, subject matter that requires significant judgment or estimation is less conducive to continuous auditing.

The second step is to evaluate the environment itself. Organizations that have environments with strong processes and controls are more conducive to continuous auditing, especially those that have continuous monitoring systems in place. It should be noted, however, that organizations do not need to have single entitywide information systems. As long as the separate systems have strong processes and controls and the IS auditor is able to retrieve and test data in a timely fashion, then it is possible to perform a continuous auditing engagement. On the other hand, the results of control testing support a low assessment of control risk. Otherwise, the extent, nature and timing of testing have to increase. The incremental effort and time needed to perform sufficient procedures would increase the cost of the engagement and reduce the derived

benefit. It also may make it more difficult for the IS auditor to meet a short reporting time period.

Continuous auditing engagements do not require new forms of testing. Traditional tests of controls and substantive tests still need to be performed. However, continuous auditing engagements require significant reliance on controls and the use of control-based testing, which can be achieved through traditional controls testing. Continuous monitoring systems may provide additional benefit to the IS auditor as these systems provide evidence on the operation of controls and the organization's ability to detect and correct error conditions on a timely basis. Substantive testing still occurs, but needs to be completed within the reporting timeframe. In the example where monthly sales and production data are reported on in a continuous basis, the IS auditor needs to access key systems and data, and capture appropriate data for analysis and testing. This includes selecting samples for controls testing as well as substantive testing of sales and production data. This example assumes that there is heavy use of data analysis tools to support the examination of sales and production data.

Finally, appropriate time periods need to be determined. There are two time periods involved. The first is the period of time that the report covers, or the reporting period. The second is the period necessary to issue a report, or the report issuance period. The reporting period is essentially definable as whatever period of time that provides meaningful data to report users. Determining the report issuance period is more complex as a number of factors go into determining what the period should be. This includes the types of systems, the time necessary for all relevant data to be entered and processed, the time required for all relevant controls and processes to operate and the time required by the IS auditor to perform control and substantive testing. In some environments the report issuance period may be very short, while in others it may be much longer. For example, if it takes a week after month-end to close the books and another week for the internal controls to detect and correct any errors and the IS auditor to perform all relevant testing, then the report issuance period is two weeks.

Obviously the quicker these processes occur, the faster a report can be issued. However, due to the extremely limited time for the internal controls to operate and the IS auditor to complete testing, there is an increased risk of material misstatement. As a result, the IS auditor may consider incorporating additional time in the report issuance period to reduce the risk of material misstatements. Ultimately the IS auditor must balance the need to provide information to users in a timely fashion against the need to ensure the audit risk is reduced to an acceptable level.

Conclusion

The implementation of continuous auditing is complex and involves many factors, however, the task is not insurmountable. There is increasing desire to provide auditing over information in a real-time (or as real-time as possible) environment. With time and effort, continuous auditing can become a reality. Demand for more reliable, relevant and timely decision-making information will create a need for continuous auditing, but the IS auditing profession needs to position itself to respond appropriately to the marketplace.

2001-2002 Standards Board of ISACA®

Chair, Claudio Cilli, CISA, Ph.D., CIA, KPMG, Italy

Claude Carter, CISA, CA, Nova Scotia Auditor General's Office, Canada

Sergio Fleginsky, CISA, PricewaterhouseCoopers, Uruguay

Alonso Hernandez, CISA, ROAC, Colegio Economistas, Spain

Marcelo Hector Gonzalez, CISA, Central Bank of Argentina Republic, Argentina

Andrew MacLeod, CISA, FCPA, MACS, PCP, MIIA, Brisbane City Council, Australia

Peter Niblett, CISA, CA, MIIA, FCPA, Day Neilson, Australia

Venkatakrishnan Vatsaraman, CISA, ACA, AICWA, CISSP, Emirates Airlines, United Arab Emirates

Sander S. Wechsler, CISA, CPA, USA

[Back](#)