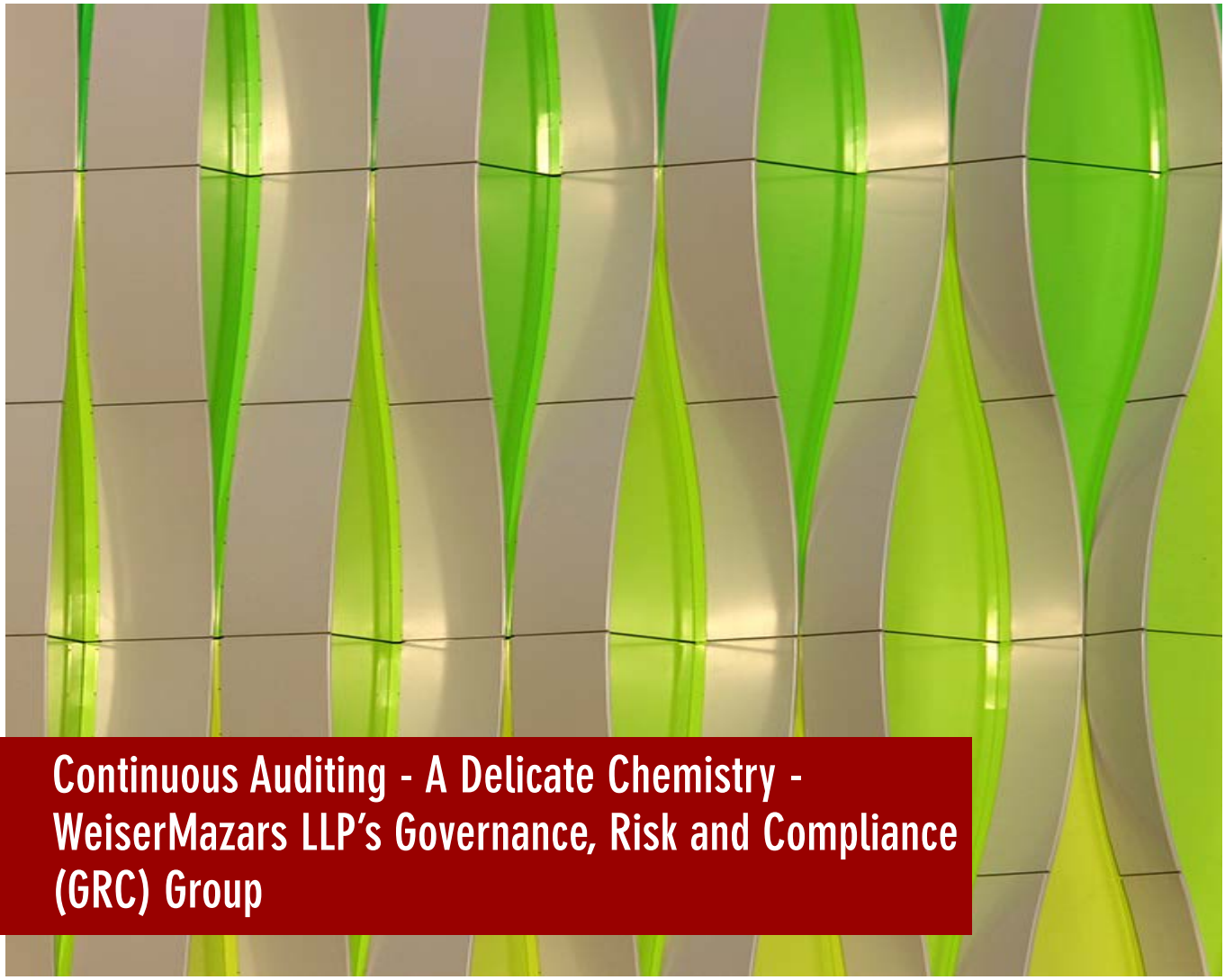
CONTINUOUS AUDITING - A DELICATE CHEMISTRY



Continuous Auditing - A Delicate Chemistry - WeiserMazars LLP's Governance, Risk and Compliance (GRC) Group

MAZARS

WeiserMazars
Exactly Right.

INTRODUCTION

Continuous Auditing (CA) has been in the minds of Audit Committees and Chief Audit Executives (CAE) for more than two decades. While the overall concept is well understood, sometimes it is confused with Continuous Monitoring (CM). A distinction between these two has to be made to understand how CA complements continuous monitoring and the unique benefits of CA. The particular approach a CAE takes in continuous auditing will be influenced by the maturity and sophistication of the organization, requiring a certain level of tailoring to achieve maximum value. We will also discuss the steps to successfully implement a continuous auditing initiative.

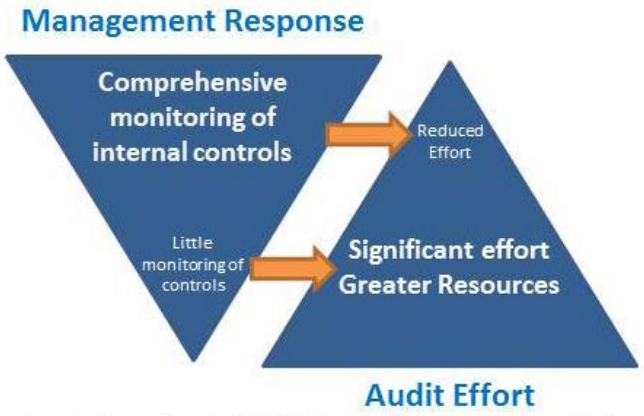
CONTINUOUS AUDITING VS. CONTINUOUS MONITORING

The concept of CA has been around for many years. The AICPA report "Special Committee on Assurance Service" mentioned it for the first time in 1995. The necessity for continuous auditing arises from a need for daily reporting and a demand for more reliable, valid and just-in-time information for effective decision-making.

Continuous Auditing - The automatic method used by persons who are able to provide assurance such as an internal auditor or an independent auditor, to perform control and risk assessments and to collect auditing evidence on a frequent basis. Continuous audit activities heavily rely on technology to automate the identification of exceptions or anomalies, analyze patterns, review trends, and test controls. Real-time continuous auditing is especially useful for high-risk enterprise processes

Continuous monitoring, in comparison, is a process under Operational management used to ensure that management's policies, procedures, and key business processes are operating effectively. CM is used as part of the control structure in the monitoring role promoted by COSO. CM detects and corrects process irregularities and helps implement process improvements (adequacy and effectiveness of internal controls). This permits ongoing insight into the effectiveness of controls and the integrity of transactions. For instance, management may identify critical control points and implement automated tests to determine, on a continuous or frequent basis, if these controls are working properly.

There are certainly similarities between Continuous Auditing and Continuous Monitoring as they both use the same automated techniques, but they are two different processes, with two different, complementary approaches. The primary difference is related to ownership of the process. Continuous monitoring is management driven (first two lines of defense) while continuous audit is audit driven (third line of defense). Although many of the continuous monitoring techniques used by management are similar to those performed by internal auditors, continuous auditing enables auditors to evaluate the adequacy of management's monitoring function and identify and assess risk areas. As the reliance by Internal Audit (IA) on the CM process increases, the assessment is not necessarily performed on a continuous basis, but more periodically as any other audits.



Inverse Relationship: Level of effort Expected by Management and Audit Activity: *Source IIA GTAC Continuous Auditing, 2005*

Another difference is in the type and sufficiency of evidence generated by continuous monitoring systems. Information provided by continuous monitoring systems can give auditors 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 IIA, in its GTAG (Global Technology Audit Guide) related to Continuous Auditing, details the CA/CM inverse relationship in regard to the amount of effort that management and the audit function put, respectively, into CM/CA. In many instances, IA led a continuous auditing initiative that was later transferred to management to become part of the continuous monitoring process. The auditor would not be part of this new control function as, in that case, his independence would be impaired.

An organization can obtain great benefits in implementing CM and CA together.

"CONTINUOUS AUDITING – THE AUTOMATIC METHOD USED BY PERSONS WHO ARE ABLE TO PROVIDE ASSURANCE SUCH AS AN INTERNAL AUDITOR OR AN INDEPENDENT AUDITOR, TO PERFORM CONTROL AND RISK ASSESSMENTS AND TO COLLECT AUDITING EVIDENCE ON A FREQUENT BASIS."

BENEFITS OF CONTINUOUS AUDITING

While continuous auditing and its benefits have been known for many years, actual implementation by the audit function has been low, although formal demands have often been made by management and audit committees. With CA, the role of the auditor can go beyond auditing procedures in which irregularities are investigated. However, this requires detailed auditing processes involving value judgments and professional skepticism.

Periodic audits no longer fit the need for continuous assurance in today's fast paced business environment. In order to adapt to this changing environment, internal audit, pushed by audit committees and supported by management, has to move to a more dynamic risk-based approach - assessing changing levels of risk on an ongoing basis, being more actively involved in risk management throughout its assessment and acting as its implementation advocate. CA results in more comprehensive and continuous assurance with greater coverage across the organization as long as the CA implementation is done consistently across primary and secondary processes. It will also enable greater accountability of the management and business owner.

Technology enables internal audit to analyze large volume of data in less time, more efficiently, while improving quality. Some practical benefits are a deeper audit for the same cost, review of exceptions only, more alternatives in choosing the approach and an increase in transparency for the auditees. To maximize its value at the earlier stages of implementation, real time CA should focus on high risk areas. The immediate benefits of CA implementation are more cost effective audits that free up resources that can be dedicated to other, more valuable areas.

This dynamics approach to risks and control as well as the redistribution of responsibilities establishes a new relationship between the audit function and management, improving the perception of the added value brought by internal audit. A better understanding of audit and management's respective priorities on risk and control issues can also be a benefit of a sound CA.

In terms of continuous auditing associated with continuous monitoring, improved areas include providing reasonable assurance that objectives of COSO ERM around reliability of reporting and compliance with laws and regulations will be met (Sarbanes-Oxley and beyond) ; better business efficiencies improving the bottom line; and increased management insight regarding risk. It also supports audit independence by ensuring that auditors have sufficient access to, and understanding of, key business information systems.

Finally, a proper implementation of CA, with clear objectives, extensive understanding of data, and properly defined outputs helps in discovering and analyzing patterns, anomalies and outliers that increase the probability of detecting fraud.

MATURITY AND SOPHISTICATION MATTERS WHICH CONTINUOUS AUDITING

Once continuous auditing has been included as an important aspect of the Internal Audit (IA) plan, with the support of management; the CAE needs to determine which point of the spectrum of continuous auditing is the most suitable for the organization. This is primarily based on the sophistication and maturity of the organization in terms of its two first lines of defense.

An organization with limited or scattered continuous monitoring will put more emphasis on continuous controls assessment as part of continuous auditing following IIA Attribute Standard 2130, which requires Internal Audit (IA) activity that assists the organization in maintaining effective controls. The continuous audit activities for this type of organization will most likely be control based, using detailed or transactional real-time or near real-time financial data. The objective is to provide control assurance to management and the audit committee. The continuous control assessment addresses not only the identification of control deficiencies, but also fraud, waste and abuse detection (covered by IIA standard 1210.A2 and AICPA SAS No 99). Because the implementation of continuous auditing might be complex (see following section) for an internal audit department with limited experience, a step-by step approach is suggested. Internal audit should start with

Computer Assisted Audit Techniques (CAATs) on some primary processes. Then, when the process is mastered move to continuous auditing. As a result, internal audit will leverage continuous auditing in order to strengthen the continuous monitoring and review environment of the organization. As many continuous auditing processes are similar to continuous monitoring techniques, internal audit may ultimately transfer the activity pertaining to continuous control assessment to become part of the control monitoring owned by management. Although the continuous auditing concept has been around for more than 20 years, many internal audit departments are still at the earliest stage of implementation, focusing on CAATs and starting to move to continuous control assessment.

Internal audit activities in more mature and sophisticated organizations with strong continuous monitoring and performance management will put less emphasis on continuous control assessment. They will perform periodic audits on the effectiveness of management's continuous monitoring. A risk based approach using continuous risk assessment will be preferred by these organizations as discussed by the IIA Standard 2120 on the evaluation of effectiveness and improvement of risk management processes. Various ongoing sets of financial and operational data will be analyzed in order to dynamically update the risk assessment and perform audit recommendation follow-ups by verifying their implementation. Analysis of trends and comparison between different periods or against a baseline will provide valuable information on risk profile evolution and identify new risks. This data driven risk assessment will dynamically impact the audit plan. The CAE might update the audit plan if risks in certain areas are evolving favorably or unfavorably. Usually, continuous risk assessment is more easily implementation when it leverages of the ERM function.

In the absence of fraud detection activities performed by management (Special Investigation Unit (SIU) for example in insurance companies), these mature organizations may perform real-time or near transactional review.

IMPLEMENTATION OF CONTINUOUS AUDITING

No matter the maturity of the organization, as with any other process/system, the continuous auditing initiative should be conducted following a step-by-step approach to achieve successful implementation.

1. Strategic plan

A strategic plan should be developed, identifying the key stakeholder, the overall objectives of the initiative, and the success criteria for measurement purposes. This document will be used for presentations to the audit committee and management.

2. Define the scope and objectives

The implementation of the CA process has to be done with a risk-based approach. As implementation can be long, it is mandatory to identify the key areas in which the implementation of CA will prove both efficient in terms of risk management and ease of implementation. To maximize the value, CA should be used to test controls, identify and assess risks and detect fraud. Once the areas have been identified, the internal audit team has to determine, with management's assistance, the controls and any continuous monitoring already in place. Like any other project, buy-in from management is essential for success. These parties need to work together to define the audit requirements, which will serve as a basis to the development and IT teams in listing the requirements for the technical solution. Although the benefits of CA are substantial, the investment in terms of time and money can be significant, especially in sophisticated and mature organizations. As such, before starting a large project many organizations use CAATs as a trampoline to continuous auditing.

One major potential road block at this stage is the absence of consensus between parties regarding the scope of the contemplated initiative. A consensus should be obtained based on well-defined objectives, explanation of the benefits, the return on investment (ROI), and a realistic scope. A too-broad scope will scare some stakeholders due to the potential for an unsustainable level of resource diversion.

3. Defining the requirements

The Chief Auditing Executive (CAE) and the internal audit team have to list controls that will be implemented to address the targeted risks. Then, the team should identify the applications containing the data needed to implement the continuous auditing solution and work along with the data owner to obtain authorization to use the data. The IT department will then be able to access the data. The access to this data will be facilitated by the support previously given by management. The internal audit team will need to understand the business processes and their supporting information systems, using existing audit and technical documentation, conducting interviews with business process owners and the IT team. The deeper the knowledge, the better the final understanding of risks and controls will be. The internal team's skills and techniques in the areas of business processes, analysis and IT systems are equally important for the success of the implementation. The control selected has to be in accordance with the internal team's technical knowledge, as well as the development and maintenance capabilities of the IT team. The frequency with which every control is performed can be set based on the risk factors.

The CAE should define the objectives of the analysis; determine a non-critical or non-complex business process that will be a pilot for the initiative. To be successful, the CAE would require an IT auditor with a sufficient knowledge of data analysis as well as a solid understanding of the organization's systems and business processes.
In addition to control testing, IA will identify fraud risks that can be detected by transactional continuous auditing. The requirements and the process will be similar to controls assessment testing. The right definition of the tests will limit the volume of false positives as well as the volume of exceptions to be investigated.

Failing to understand the business processes or a lack of necessary technology skills in IA could dramatically impact the outcome of the project and lead to significant cost and time overrun.

4. Retrieving and Using Data

Once the project team has defined the scope, the objectives, and the requirements, the next step is to retrieve and use the data. The technology that will be used by the auditor to automate the analysis should be carefully chosen to ensure success. The main drivers of this selection are the type of data source (existence of interface, ETL), the volume of data to be analyzed, format (old format or proprietary), and with the recent advent of Big Data, velocity (timely capture of data). The software should also be scalable and flexible enough to accept new sources of data.

Access to data with the appropriate rights (read only) will be given to the audit team. Depending on the objectives, the access level would vary from database access (dump), to running queries, scripting and reporting platform access. Retrieving data from the source system should not impact production. The auditor will ensure throughout the process the completeness and integrity of the data retrieved, and checks will be done before and after the transfer to the auditor. The set of data will be analyzed through repeatable tests with a software package such as ACL, IDEA, or SaaS. Scripts and routines should be developed in order to speed up the analysis.

The timeliness of data as well as the frequency of the data retrieval should be aligned with the project objectives. Obtaining data is one of the most common challenges in continuous auditing projects. More often than not, the auditor is faced with data that is incomplete, inconsistent, or not accessible due to its confidentiality (HIPPA, PII). The atomicity of system source in case of a decentralized IT environment is also challenging. Big Data has added another layer of complexity, increasingthe difficulty of identifying the appropriate data and not being overwhelmed by sheer volume.

These challenges can be overcome by precisely defining, at the earliest stage of the project (during requirements), the data sets that need to be accessed. This requires having a deep knowledge of the organization's systems, database and data confidentiality. More importantly, data owners should be part of the team. The IA should not seek more data than needed (i.e. excessive data granularity that will not be necessary for the tests).

5. Analysis and reporting

Based on the sophistication and maturity of the organization, the analysis will be conducted for the purpose of continuous control assessment, transaction level testing for fraud detection purposes, continuous risk assessment, or a combination of these three elements (continuous auditing spectrum). The set for the analysis will be defined in order to meet the objectives. It could encompass trends, rule based exception reports, comparisons, clustering and so on.

The results of the analysis should be prioritized base on the risk profile. Usually, they are sent to business process owner for investigation of the exceptions found. This process would be done iteratively in order for the team to be increasingly conformable and the scope expanded to other areas.

The final results is then part of the overall risk assessment, reported to the audit committee.

Common risks at this stage are inconsistent or inappropriate design of the analysis (inappropriate frequency, set of data, test not aligned with objectives, etc.) or misinterpretation of the results (false positive, misunderstanding of data, lack of understanding of the risk). These risks are usually addressed by a proper alignment with objectives and a deep understanding of the risks/controls to be tested/assessed.

6. Measurement

Internal audit departments are often challenged by management regarding the ROI of the continuous auditing initiative. As part of the project, the team should define and implement Key Performance Indicators in order to provide to management objective results that will be compared will predefined criteria. This will help demonstrate, if the continuous auditing initiative is implemented and executed properly, the savings (costs and time) and benefits. These criteria could include risk assessment evolution, level of assurance per risk (manual testing vs automated testing), number of controls tested, number of exception reported, time saving in audits, or reallocation of time to added value audits.

CONCLUSION

The road to a successful implementation of continuous auditing is full of challenges. All project stakeholders need to understand what their responsibilities are in the continuous auditing and continuous monitoring processes and where these processes will be implemented. While the true ROI of the initiative will not be measured in the short term, the value of continuous auditing, no matter the maturity or sophistication of the organization, is demonstrated over time by measurement against objective criteria - the early detection of fraud and the timely adaptability by IA to emerging risks. Full buy in by management, detailed planning and strong alignment between defined requirements (data and resources) and organizational objectives are key to a successful implementation. Finally, deep technology knowledge and understanding of the organization's information system by the IA team is equally critical.

CONTACT

Bill Mellon, Partner
(P) 267.532.4328 (C) 215.287.0468
(E) Bill.Mellon@WeiserMazars.com

Nicolas Quairel, Principal
(P) 646.225.5983
(E) Nicolas.Quairel@WeiserMazars.com

About WeiserMazars

WeiserMazars LLP provides insight and specialized experience in accounting, tax and advisory services.

Since 1921, our skilled professionals have leveraged technical expertise and industry familiarity to create customized solutions to overcome client challenges.

As the independent U.S. member firm of Mazars Group – the 11th largest accounting organization in the world – we have a global reach of nearly 14,000 professionals in more than 70 countries.

Locally and internationally, we build lasting relationships with our clients by addressing their particular needs, creating value and optimizing their organizational performance.

For more information visit us at www.weisermazars.com

Follow us on