# Table of Contents

Purpose........................................................................................................................................... 1  
Background ................................................................................................................................... 1  
Definitions ...................................................................................................................................... 2  
Continuous Auditing – Professional Expectations ................................................................. 2  
Linking Continuous Auditing to Departmental Expectations .............................................. 3  
Monitoring Roles ....................................................................................................................... 4  
Continuous Auditing – Establishing the Objective ................................................................. 5  
Implementation Considerations ................................................................................................. 5  
An Approach to Developing a Continuous Auditing Application ........................................ 6  
Conclusion ..................................................................................................................................... 10  
Appendix A – Example of Continuous Auditing: Accounts Payable Audit ................. 12
Purpose

This document provides chief audit executives (CAEs) and internal auditors with guidance on developing a continuous auditing application. It describes an incremental approach to the development of a continuous auditing application for federal internal auditors, one that builds on the existing risk-based audit planning process and the results of completed audit engagements. It encourages a focus that not only increases the efficiency and effectiveness of the internal audit process but also improves risk management and control processes by enhancing management’s monitoring capabilities.

Background

Traditionally, internal audit’s testing of controls has been performed on a retrospective basis, often many months after business activities have occurred. The testing procedures have typically been based on a sampling approach and included activities such as reviews of policies, procedures, approvals, and reconciliations. To remain relevant, internal auditors need to move beyond a static, cyclical approach and adopt a continuous, comprehensive approach to audit and risk assessment — an approach that optimizes the use of technology. To enhance the value added by internal auditing practices, many successful audit groups are benefiting from the enhanced use of continuous auditing as a method to perform control and risk assessments more efficiently and more frequently.

Continuous audit practices change the audit paradigm from periodic reviews of a sample of transactions to ongoing testing of 100 percent of the transactions. Continuous auditing allows auditors to better understand risks as well as critical control points, rules and exceptions. They can analyze key business systems for both anomalies at the transaction level and for data-driven indicators of emerging risk and control weaknesses. Finally, continuous auditing can be integrated into all aspects of the audit process, from the development of the risk-based audit plan to the conduct and follow-up of specific audits.

According to a 2009 survey of CAEs, technology will have a major impact on internal audit. Among the different types of technology, continuous auditing, data analysis, and fraud prevention and detection are considered to be the most important. The problem faced by CAEs is that the notion of continuous auditing tends to raise expectations that can be difficult to deliver on. This is primarily because of the confusion surrounding continuous auditing. A related source of confusion is the similarities and differences between continuous auditing and continuous monitoring. It is, therefore, extremely important to manage expectations by developing an understanding of what continuous auditing is and what it will and will not do. This will help CAEs identify and communicate objectives for continuous auditing that are clear and achievable.
Definitions

**Assurance** is an opinion of the state of affairs — about overall financial performance or a specific transaction, governance process, or risk. Audit assurance is an independent statement about the adequacy and effectiveness of the risk management and control processes and the integrity of information.

**Continuous assurance** is achieved through the combination of the continuous auditing activities performed by internal audit to independently evaluate the state of the risk management and control processes, and the continuous monitoring activities performed by management.

**Continuous auditing** is any method used by audit to perform audit-related activities on a more frequent basis. It includes continuous control assessments and continuous risk assessments. Typically, the frequency is based on the inherent level of risk in the item being audited; and the continuous auditing approach relies heavily on technology.

- **Continuous control assessment** refers to activities used by auditors to assess the controls. It allows internal auditors to provide independent assurance that the controls are working effectively and that the organization can respond quickly to correct deficiencies that arise.

- **Continuous risk assessment** refers to activities used by auditors to identify and assess the level of risk. It enables auditors to identify emerging areas that place a department at risk, to prioritize such risks, and to more effectively allocate limited audit resources. However, these activities do not in any way preclude management’s responsibilities to perform a monitoring function and manage risk.

**Continuous monitoring** encompasses the processes that management puts in place to ensure that policies, procedures, and business processes are operating effectively. It addresses management’s responsibility to assess the adequacy and effectiveness of controls.

**Continuous Auditing – Professional Expectations**

Today’s internal auditors do not just audit control activities; they also keep an eye on the organization’s risk profile and play a key role in identifying areas to improve risk management processes.¹ In some areas, such as financial systems, there may be synergy with continuous monitoring processes, whereas other elements of high risk may not have active monitoring programs. For key risk-based areas, the CAE must be able to provide senior management with ongoing assessments of the health of internal controls and the levels of risk within an organization.

The Treasury Board Policy on Internal Audit states that internal audit “provides objective, substantiated conclusions as to the functioning of the organization’s risk management, control,
and governance processes.” Further, as an adjunct to the assurance role, internal audit is expected to offer solutions-oriented recommendations; accordingly, internal audit has an important role to play in evaluating risks and controls.

The Institute of Internal Auditors’ (IIA) Practice Advisory 1210-1 states that an internal auditor’s knowledge, skills, and competencies should include “knowledge of key information technology risks and controls and available technology-based audit techniques.” IIA Standard 1220.A2 states that “internal auditors must consider the use of technology-based audit and other data analysis techniques.” In addition, IIA Standard 2120 states that audit “must evaluate the effectiveness and contribute to the improvement of risk management processes.” Standard 2130 provides a similar statement about controls: “Auditors must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.”

To fulfill these obligations, informed CAEs are using all means available, including advances in technology, data analytics, and electronic information. When effectively implemented, continuous auditing uses dynamic thresholds and risk drivers to support both the ongoing identification and assessment of risk and the assessment of controls. This adds value, not only for the provision of assurance but also for the timely identification of increasing risks and control breakdowns.

**Linking Continuous Auditing and Departmental Expectations**

The Treasury Board Policy on Internal Controls states that the deputy head is responsible for

...ensuring the establishment, maintenance, monitoring, and review of the departmental system of internal control to mitigate risks in the following broad categories:

- The effectiveness and efficiency of programs, operations and resource management, including safeguarding of assets;
- The reliability of financial reporting; and
- Compliance with legislation, regulations, policies, and delegated authorities.

Further, as a result of the development and revision to policies under the policy suite renewal, many Treasury Board policies contain monitoring and reporting requirements. The revised policies often require that departments have processes in place for assessing risk and for the design, implementation, and ongoing maintenance of controls within the organization. Also, to meet the requirements of the revised policies, TBS must actively and constructively engage senior departmental managers, including internal audit and evaluation managers, to develop, using a risk-based approach, a government-wide understanding of the state of management practices and controls.

Ideally, because of concerns about the burden of compliance, efforts, and the scarcity of resources, a department will institute a combined strategy of continuous monitoring and continuous auditing to demonstrate that monitoring requirements are met.
Monitoring Roles

Departmental management is expected to ensure that policies, procedures, and processes are operating effectively. Meeting this requirement likely includes forms of continuous monitoring, which may use techniques similar to those used by internal auditors, such as highlighting transactions that may not comply with control objectives or assertions.

There is, however, a fundamental difference between the tests performed by management and those performed by internal audit. Management has the primary responsibility for assessing risk and for the design, implementation, monitoring and ongoing maintenance of controls within an organization. The purpose of management’s monitoring process, therefore, is to provide those responsible for the controls systems, such as the chief financial officer and the deputy head, with support for attestations or assurances that risk and control functions are operating as intended. Internal audit is responsible for assessing the adequacy and effectiveness of the organization’s risk management system and the control frameworks. The purpose of internal audit’s continuous auditing processes is to support an independent opinion of the adequacy and effectiveness of the organization’s risk management system and the control framework implemented by management.

The adequacy of the proactive monitoring performed by management will directly affect how auditors approach continuous auditing. Where the continuous monitoring is being performed by management, a high level of detailed transaction testing may not be required under continuous auditing. Instead, auditors can examine the effectiveness of management’s monitoring to ensure that the management monitoring process is still adequately addressing the risks and testing key controls. Depending on the outcome of such tests, the scope, level of detail, and frequency of audit testing would be adjusted accordingly.

When management monitoring systems do not exist, internal audit may be asked to develop continuous auditing applications to support the department’s monitoring requirements. In such cases internal audit should strive to develop continuous auditing tests that are then handed over to management to use as the beginning of a continuous management monitoring system. While this may be an initial means of introducing monitoring programs, IIA Standard 2120 warns that “when assisting management in establishing or improving risk management and control processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.” In particular, the involvement of internal audit must exclude determining the corporate risk appetite.
Moreover, when management assumes responsibility for a continuous auditing application developed by internal audit, management should not simply adopt the processes and tests used by internal audit. Instead, management should conduct an independent review of the risks and controls to ensure that the monitoring application meets their monitoring needs.

Management’s use of continuous monitoring procedures, together with a complementary continuous auditing program, typically satisfies demands for assurance that control procedures are effective and that information provided for decision making is both relevant and reliable.

**Continuous Auditing – Establishing the Objective**

In developing the objective for continuous auditing, the CAE must ensure that continuous auditing is not confused with “continuously performing the same audit.” Continuous auditing refers to the ongoing assessment of control framework and risk management systems.

Continuous auditing provides internal auditors with an opportunity to go beyond the confines of traditional audit approaches and the limitations of sampling, reviews of standard reports, and point-in-time assessments. The power of continuous auditing lies in the intelligent and efficient testing of controls and risks that results in timely notification of gaps and weaknesses to allow immediate follow-up and remediation. By changing their overall approach in this way, auditors will develop a better understanding of the business environment and the risks to the department or agency to support compliance and drive the achievement of objectives.

A reasonable objective for continuous auditing would be to use technology-enabled analyses that contribute to the efficiency and effectiveness of the audit process and the improvement of risk management and control processes. This can accomplished through the performance of audits identified in the risk-based audit plan, and the conduct of data analyses during, and after the completion of, the specific audit. Together, these activities seek to identify and assess changing levels of risk and the adequacy and effectiveness of controls.

**Implementation Considerations**

**Continuous Auditing Functionality**

Continuous auditing has a wide range of functionalities that support audit activities and the CAE through enabling methodologies and services that include:

- risk management strategies and practices — by identifying and assessing risks early;
- management control framework reliability — by highlighting control weaknesses;
- information for decision making — by examining the reliability and accessibility of the information used by managers;
- the selection of audit projects for inclusion in the annual audit plan — by identifying areas of higher risk;
the implementation of timely and effective corrective actions — by verifying the implementation of audit recommendations; and
the identification of audit engagement scope and objectives – by better understanding the business process and associated risks and mitigating controls.

The implementation of continuous auditing will not be the same in every department. Therefore, when developing the objectives for continuous auditing, the CAE must determine the nature and extent of what is to be accomplished. When defining the strategy for continuous auditing, the objectives and approach should be vetted by senior management and presented to the departmental audit committee. In addition, the concept of continuous auditing should be referenced in the internal audit charter.

Outlining the strategy for continuous auditing with management and obtaining audit committee endorsement are critical to the program’s success, as is ensuring that the application complements management’s monitoring role. The following factors should be considered when determining internal audit’s ability to develop a successful continuous auditing application:

- the availability and integrity of the data to support continuous auditing
- the adequacy of resources (hardware, software, and people)
- the importance of developing standards, practices, and procedures around the analysis to be performed to ensure that consistency increases the assurance provided through the application
- the need to manage the use of continuous auditing — ensuring that a proper plan and objectives exist and that results are monitored and tracked
- the assignment of responsibilities for leadership, program management, data management, quality assurance, and technical support
- the establishment of a structure for managing, protecting, and sharing analysis routines and results
- the importance of providing for the ongoing skills development of the auditors
- the maximization of technology to improve audit efficiency and effectiveness

An Approach to the Development of Continuous Auditing

Where to Begin

But where does one begin? Too often auditors get started on the wrong foot, such as trying a “bottom-up” approach to identify all the controls, and are then unable to take the necessary steps to put continuous auditing into practice. Lessons learned through the Sarbanes-Oxley era noted that a “top-down” approach to key control identification is more efficient and valuable. Focussing on key strategic risk areas, then highlighting requisite controls for testing, was found to be as effective as trying to document and test all key controls. The same approach can be adopted in the development of a continuous auditing application. However, unless the department’s auditors have already been using data analysis techniques to support regular audit engagements, they probably do not even have access to the data; they do not know whether the
data can be relied on; and they may not know the primary business risks and which controls are key. The task can still seem overwhelming.

It is, therefore, important to think of continuous auditing from an integrated perspective: people and process issues, such as appropriate skills, training, experience, and to define roles and responsibilities, in addition to considering audit software, technology, and information systems. To do this, auditors need to develop an understanding of the areas of risk, the business processes, the supporting information systems, and the underlying data and automated controls.

It is recommended that continuous auditing be introduced incrementally: starting with its use within audits; then following progress regarding audit recommendations; and finally creating periodic, repetitive analysis of key risk indicators. When sufficient confidence in the application is gained, the concepts should be introduced into high-level risk identification and audit planning. Figure 2 provides an overview of this audit engagement-based approach.

**FIGURE 2 – Approach to Continuous Auditing**

This approach allows for enhanced testing of the adequacy and effectiveness of risk and control mechanisms. If done correctly, continuous auditing will support more accurate and timely reporting about the adequacy and effectiveness of controls. The results of audits will clearly
identify key business risks and the mitigating controls for the area being audited, the source of the data, and the analyses to be performed. The auditor will also establish indicators and baseline measures against which future analyses should be evaluated.

**The Risk-Based Audit Plan**

In selecting which areas to audit, the CAE should identify critical business processes by categorizing and rating risk areas. The departmental risk profile, interviews with business process owners, and the results of other assurance providers are all excellent sources of information on risks that should be considered.

The selection of continuous auditing areas typically flows from the annual risk-based audit plan. The risk-based audit plan identifies and ranks the risks facing an organization and identifies specific audits to assess these risks; as such, it is an excellent source of information about specific risk areas and the associated audits.

The risk-based audit planning process will also identify areas where it would be useful to obtain additional information supporting the identification and assessment of risk and where an audit may be used to obtain this information. The team leader for these audits should be informed of the need to identify and assess risk drivers during the conduct of the audit.

Once the risk-based audit plan has been approved, the first step in developing continuous auditing is to define the appropriate subject area. Factors to consider in determining whether continuous auditing is appropriate for the selected audit include the following:

- **Audit objectives:** While the audit objectives may be fairly broad, the specific area selected for the development of a continuous auditing application may be more narrowly defined. For example, attempting to perform continuous auditing on the entire set of financial statements for a large department with disparate information system is virtually impossible. However, addressing key financial risks and controls for a single information system may be much easier. Indeed, the more specific the subject area, the more conducive it may be to continuous auditing.

- **Buy-in:** The CAE should also consider whether support for continuous auditing can be obtained from the business process owner.

- **Benefits:** Not all audits are a good starting point for developing continuous auditing. The CAE must develop criteria for determining whether an audit is appropriate for contributing to the development of continuous auditing. The criteria include critical business processes, key business risks and controls, availability and integrity of data, and the costs or benefits and the ramifications of using continuous auditing on the selected area.

**The Audit Engagement**

The development of a continuous auditing application should be an ongoing process that starts with auditors obtaining access to, and verifying the integrity of, the data. Typically, this activity
is done within the context of a specific audit. When fulfilling their specific audit objectives, the audits selected to support the development of continuous auditing provide an opportunity for the internal auditors to work with business process owners and to

- develop a detailed understanding of the business processes;
- identify the key risks and mitigating controls;
- identify the underlying information systems and obtain necessary access;
- verify the reliability of the analyses and the data;
- develop a detailed understanding of the supporting data;
- assess the existence and adequacy of the mitigating controls;
- ensure the development of performance measures for key business risks and rules for key controls;
- establish baseline measures and thresholds for exception reporting;
- build and test continuous auditing routines;
- determine when and how often the continuous auditing tests will be run;
- run analysis routines;
- develop monitoring and reporting mechanisms; and
- monitor and assess effectiveness of the continuous auditing application.

Furthermore, auditors should consider the mix of continuous auditing objectives (deterrent, detective, or preventive) that will be developed through the audit procedure and their applicability to the audit objectives.

This approach to the development of a continuous auditing application has immediate benefits because the analyses support current audits, making them more efficient and effective, and allow auditors to get valuable experience in accessing, assessing, and analyzing the data. Through the individual audits, auditors will also develop contacts with the business system owners and programmers. These contacts will allow auditors to get insight into the risks and mitigating controls and to establish protocols for the communication of continuous auditing results.

At the completion of the audit, the auditor should work with the business process owners when developing a continuous auditing application. Discussions might include obtaining input on the frequency and length of the continuous auditing activity, as well as the specific tests to be run, and how the results could be communicated to management. Audit must maintain sufficient independence when developing and implementing a continuous auditing application, but should also seek to ensure its utility in support both audit’s risk-based planning and management’s risk management processes.

**Follow-up – Monitoring Actions**

Additional analyses should be run as part of a follow-up to the audit to ensure that management actions have been taken and are having the desired effect. This would be evident by a change in
the identified measures when compared to the baseline levels. The analyses would be run periodically to determine if key indicators were changing, reflecting increases or decreases in the levels of risk.

**Ongoing Use of Continuous Auditing**

The use of ongoing audits to develop continuous auditing routines serves a number of complementary purposes including the assessment of the implementation of management action plans to address the audit’s recommendations; the ongoing monitoring of risk measures (and the possible launch of a follow-up audit); the testing of the adequacy of mitigating controls; and input into audit’s risk-based audit planning process.

The next phase in the development of a continuous auditing application is often the creation of repetitive or periodic analyses, often linked to repeat audits. These types of analyses seek to improve the efficiency and effectiveness of the audit function by addressing the objectives of recurring audits. The continuous auditing application would build on the queries developed to address specific audit objectives.

At this phase the analytics are often managed by a specialist and deployed to audit staff on an “as-needed” basis. The final phase is the continual execution of audit tests to identify risks, as well as the timely identification of errors, anomalies, patterns, and exceptions. This phase supports individual and repeat audits as well as the ongoing risk and control assessments. The frequency and duration of the continued running of these tests as part of a continuous auditing application will depend on the level of risk. Once the risk mitigation is in place, and management monitoring is being performed, the extent of continuous auditing in the area can be decreased; and continuous auditing efforts can focus less on detailed testing and more on assessing management’s monitoring process.

**Conclusion**

Heightened expectations of internal audit, coupled with enhanced data analysis technology, have caused fundamental changes in audit’s approach by allowing entire populations of financial and operational transactions and other data to be comprehensively tested and, where appropriate, to be analyzed in close to real time. Therefore, the internal audit profession is turning to continuous auditing as an effective and efficient means of delivering assurance services.

The development of a continuous auditing application requires a structured approach. It should be linked to the risk-based audit planning process, and leverage existing audit projects. (Appendix A provides an example.) Further, continuous auditing relies heavily on audit’s access to and ongoing efforts to understand and use information from a variety of business systems. The intelligence that auditors gain from the use of data analysis to support individual audits can improve the overall risk management and control processes.

Continuous auditing should be considered as a process, not an end state. The process must be fluid and allow for constant changes. For example, the amount of detailed testing by internal audit will ebb and flow depending on the results of audit’s assessment of management’s
monitoring process and the emergence of new risks. Audit may start by performing detailed testing in an area on a regular basis; transition to verifying the management’s monitoring function and only performing limited periodic testing; and then, as a result of new risks, initiate additional detailed testing again. For this reason, internal audit must constantly examine not only management’s monitoring function but also the changing risk exposures.

The evolution towards continuous auditing will take time and attention from the CAE as well as additional costs and resources as continuous auditing activities are implemented and sustained. Consequently, CAEs planning to implement a continuous auditing approach need to be willing to move beyond their traditional auditing approaches and techniques. They must fully integrate continuous auditing in risk-based planning activities, control testing routines as well as audit conduct, reporting, and follow-up phases. Continuous auditing is not something to do in addition to the usual audit activities; it must be part of ongoing audit operations. Finally, continuous auditing should support management monitoring by contributing to the risk management and control processes.
Appendix A – Example of Continuous Auditing: Accounts Payable Audit

During the interviews supporting the development of the annual risk-based audit plan, the accounts payable manager raised concerns over the risks related to the improper understanding of the payment on due date policy by the clerks, the proper separation of duties, and the effectiveness of the automated controls over commitment accounting. There was a reliance on the SAP application controls, and the manager was concerned about their effectiveness. Some of the identified risks had not been included in the preliminary objectives for the audit; however, the audit team leader felt that they were consistent with the overall audit objective and should be included.

The auditors obtained access to the financial system and assessed the integrity of the data. Next, specific tests were developed as part of the audit to identify risk drivers and measures and to assess the risks and control weaknesses, such as

- payment on due date — an analysis of number and dollar value of payments by payment terms (immediate and 15, 30, 60, and 90 days);
- separation of duties — an analysis to verify that goods receipts and invoice receipts were entered by different persons and that, under section 33 of the *Financial Administration Act*, the user was not also a payee on any transaction; and
- commitment accounting — an analysis to determine if invoices for $20 thousand or more were referenced to a purchase order or requisition

The analysis confirmed high levels of risk in these areas and established baselines for each test.

The audit included steps for assessing the adequacy of the continuous monitoring performed by management. The management monitoring process included tests of the financial application’s controls over the payment of duplicates, and the review by the accounts payable manager of a report detailing potential duplicates. The auditor tested the controls over duplicate payments and found these to be adequate and management’s monitoring of potential duplicates to be effective.

Given the favourable assessment of the monitoring process, the auditors concluded that an analysis run quarterly to measure the total dollar value of potential duplicates would be sufficient. If the total value of potential duplicates remained below threshold values, then an audit could safely conclude that the controls and monitoring processes were still working and that additional detailed transaction testing was not necessary. However, if the results indicated that there was a problem with duplicate payments, the auditors would perform more detailed tests to assess the effectiveness of the controls and to identify weaknesses.

The auditors decided that the accounts payable area would benefit from the development of additional continuous auditing routines. The data was readily available and had sufficient integrity, and the accounts payable manager was receptive to the idea. Specific tests were identified and run on a quarterly basis, the results were provided to the accounts payable manager for corrective action. The accounts payable manager also established a plan to develop a monitoring program that would be implemented next fiscal year. The accounts payable...
manager planned and assumed responsibility for the analyses performed by audit when developing the monitoring plan.

In the above example, an accounts payable audit was used to obtain access to the financial data and test its reliability; to examine the business processes and the related risks; to identify risk drivers for significant risks and assess key controls; and to validate the analysis results. The audit also assessed the management monitoring process. The knowledge gained from the audit was then used to develop the beginnings of a continuous auditing application that would be run by the auditors until management’s monitoring program was adequately in place.