

GTAG

GLOBAL TECHNOLOGY AUDIT GUIDE

**Continuous Auditing:
Implications for Assurance,
Monitoring, and
Risk Assessment**



The Institute of
Internal Auditors



“There is increasing scrutiny over IT controls with Sarbanes-Oxley. I can meet the auditor’s security requirements cost-effectively with BindView.”

Eric Craig
Managing Director
Infrastructure Engineering
Continental Airlines

CLEARED FOR TAKEOFF.

SARBANES-OXLEY

Compliance Success: Continental Airlines

VISIT US AT WWW.SEARCHSECURITY.COM/BINDVIEW TO DOWNLOAD A NEW IDC WHITE PAPER, “HOW TO REDUCE THE COST OF SECURITY COMPLIANCE.” OR CALL US TOLL-FREE AT 1-800-813-5869.



THE BEST
SECURITY COMPLIANCE
SOLUTION FOR YOUR BUSINESS.

Continuous Monitoring. Continuous Auditing. Continuous Assurance.



In today's regulatory environment, chief audit executives are finding that their departments are becoming more and more consumed with the monitoring and testing of internal controls to meet the demands of compliance. Yet, a multitude of operational and financial audit activities remain. Many internal audit departments are turning to technology to ease the burden by increasing efficiencies and productivity and to drive business performance.

This Global Technology Audit Guide (GTAG) "Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment" provides guidance for CAEs on how to implement an ideal strategy combining continuous auditing and continuous monitoring solutions to address these challenges. ACL's data analytics technology and Continuous Controls Monitoring solutions leverage best audit practices to satisfy today's heightened demands for effective controls. ACL can help you demonstrate the benefits of appropriate technology investments – while supporting ongoing compliance requirements, increasing operational effectiveness, and contributing to the bottom-line.

ACL is pleased to have been a contributor and the sponsor of this valuable and informative resource.

GTAG Partners



AICPA – American Institute of
Certified Public Accountants
www.aicpa.org



CIS – Center for Internet Security
www.cisecurity.org



CMU/SEI – Carnegie-Mellon University
Software Engineering Institute
www.cmu.edu



ISSA – Information Systems Security Association
www.issa.org



ITPI – IT Process Institute
www.itpi.org



NACD – National Association of
Corporate Directors
www.nacd.org



SANS Institute
www.sans.org

Global Technology Audit Guide
Continuous Auditing:
Implications for Assurance,
Monitoring, and Risk Assessment

Author

David Coderre, Royal Canadian Mounted Police (RCMP)

Subject Matter Experts

John G. Verver, ACL Services Ltd.

J. Donald Warren Jr., Center for Continuous Auditing, Rutgers University

GTAG – Table of Contents

- 1. Summary for Chief Audit Executive1
 - Continuous Auditing1
 - The Need for a Continuous Auditing/Continuous Monitoring: An Integrated Approach1
 - The Roles of Internal Audit Activity and Management2
 - The Power of Continuous Auditing2
 - Implementation Issues2
- 2. Introduction3
 - Continuous Auditing: A Brief History3
 - Today’s Audit Environment3
 - COSO Enterprise Risk Management (ERM) Framework4
 - The Roles of the Internal Audit Activity and Management5
 - Benefits of Continuous Auditing and Monitoring5
- 3. Key Concepts and Terms: The Need for Clarity7
 - Continuum of Continuous Auditing8
- 4. Relationship of Continuous Auditing to Continuous Assurance and Continuous Monitoring9
 - Continuous Assurance9
 - Continuous Monitoring9
 - Continuous Auditing9
- 5. Areas for the Application of Continuous Auditing11
 - Applications for Continuous Control Assessment11
 - Applications for Continuous Risk Assessment13
 - Development of Audit Plan14
 - Support to Individual Auditing15
 - Follow-up on Audit Recommendations15
 - Conclusion16
- 6. Implementing Continuous Auditing17
 - Continuous Auditing Objectives17
 - Continuous Control and Risk Assessment – Relationship21
 - Manage and Report Results23
 - Challenges and Other Considerations24
- 7. Conclusion26
- 8. Appendix A – Example of Continuous Auditing Applied to Accounts Payable27
- 9. Appendix B – Related Standards29
- 10. Appendix C – Continuous Auditing Self Assessment30
- 11. About the Author32
- 12. References33

The need for timely and ongoing assurance over the effectiveness of risk management and control systems is critical. Organizations are continually exposed to significant errors, frauds or inefficiencies that can lead to financial loss and increased levels of risk. An evolving regulatory environment, increased globalization of businesses, market pressure to improve operations, and rapidly changing business conditions are creating the need for more timely and ongoing assurance that controls are working effectively and risk is being mitigated.

These demands have put increased pressure on chief audit executives (CAEs) and their staff. Internal audit departments have been extensively involved in a wide range of compliance efforts, particularly due to legislation, such as Section 404 of the U.S. Sarbanes-Oxley Act of 2002, raising concerns not only about mounting expectations, but also about internal auditors' ability to maintain independence and objectivity when evaluating the effectiveness of controls, risk management, and governance processes.

Today, internal auditors face challenges in a range of areas:¹

Regulatory Compliance and Controls: Evaluation and identification of issues and processes, sustainability, resources, defining materiality, priorities, and financial reporting risks.

Internal Audit Value and Independence: the high expectations of internal auditing, growing internal controls issues, confusion around the role of internal auditing liability and responsibility, and compromised objectivity and independence.

Fraud: Detection and control, identity theft, fraud management responsibility, and increased incidence and cost of fraud.

Availability of Skilled Resources: Lack of competency and appropriate skill sets, shortage of auditors, retention, and lack of understanding of risks and controls.

Technology: appropriate solutions to support compliance, technology business model, information security, competing information technology (IT) priorities, and outsourcing.

It is evident that a new approach, one that provides a sustainable, productive, and cost-effective means to address these issues, is essential.

Continuous Auditing

Traditionally, internal auditing's testing of controls has been performed on a retrospective and cyclical basis, often many months after business activities have occurred. The testing procedures have often been based on a sampling approach and included activities such as reviews of policies, procedures, approvals, and reconciliations. Today, however, it is recognized that this approach only affords internal auditors a narrow scope of evaluation, and is often too late to be of real value to business performance or regulatory compliance. Continuous auditing is a method used to perform control and risk assessments automatically on a more frequent basis.

Technology is key to enabling such an approach. Continuous auditing changes the audit paradigm from periodic reviews of a sample of transactions to ongoing audit testing of 100 percent of transactions. It becomes an integral part of modern auditing at many levels. It also should be closely tied to management activities such as performance monitoring, balanced scorecard, and enterprise risk management (ERM).

A continuous audit approach allows internal auditors to fully understand critical control points, rules, and exceptions. With automated, frequent analyses of data, they are able to perform control and risk assessments in real time or near real time. They can analyze key business systems for both anomalies at the transaction level and for data-driven indicators of control deficiencies and emerging risk. Finally, with continuous auditing, the analysis results are integrated into all aspects of the audit process, from the development and maintenance of the enterprise audit plan to the conduct and follow-up of specific audits.

The Need for Continuous Auditing/Continuous Monitoring: An Integrated Approach

In light of CAEs' concerns regarding the burden of compliance efforts, the scarcity of resources, and the need to maintain audit independence, a combined strategy of continuous auditing and continuous monitoring is ideal.

Continuous monitoring encompasses the processes that management puts in place to ensure that the policies, procedures, and business processes are operating effectively. It addresses management's responsibility to assess the adequacy and effectiveness of controls. This involves identifying the control objectives and assurance assertions and establishing automated tests to highlight activities and transactions that fail to comply. Many of the techniques of continuous monitoring of controls by management are similar to those that may be performed in continuous auditing by internal auditors.

Management's use of continuous monitoring procedures, in conjunction with continuous auditing performed by internal auditors, will satisfy the demands for assurance that control procedures are effective and that the information produced for decision-making is both relevant and reliable.

An important additional benefit to the organization is that instances of error and fraud are typically significantly reduced, operational efficiency is increased, and bottom-line results are improved through a combination of cost savings and a reduction in overpayments and revenue leakage. Organizations that introduce a continuous auditing and controls monitoring approach often find that they achieve a rapid return on investment.

The business and regulatory environment and emerging audit standards are driving auditors and management to make more effective use of information and data analysis technologies as a fundamental enabler of continuous auditing and continuous monitoring.

¹ Report from The IIA's 2005 International Conference CAE Roundtable Discussion, July 2005.

GTAG — Summary for the Chief Audit Executive — 1

The Roles of Internal Auditing and Management

Management has the primary responsibility for assessing risk and for the design, implementation, and ongoing maintenance of controls within an organization. The internal audit activity is responsible for identifying and evaluating the effectiveness of the organization's risk management system and controls as implemented by management. Auditors conduct the evaluation to provide assurance to the audit committee and senior management as to the state of risk and control systems and, in the case of legislation such as the Sarbanes-Oxley Act, the reliability of management's representation concerning the state of controls. Ideally, internal auditing is not part of the controls monitoring process and does not design or maintain the controls, thereby retaining its independence.

Although the monitoring of internal controls is a management responsibility, the internal audit activity can use and leverage continuous auditing to strengthen the overall monitoring and review environment in an organization. The level of proactive monitoring performed by management will directly affect how auditors approach continuous auditing. In cases where the continuous monitoring of controls is being performed by management, the same level of detailed transaction testing may not be required under continuous auditing. Instead, auditors can focus on procedures to determine the effectiveness of management's monitoring process and, depending on the outcome of such tests, adjust the scope, number, and frequency of audit testing.

The Power of Continuous Auditing

The power of continuous auditing lies in the intelligent and efficient continuous 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 company to support compliance and drive business performance.

Implementation Issues

The CAE must be cognizant of the fact that continuous auditing will change the audit paradigm, including the nature of evidence, timing, procedures, and level of effort required by internal auditors. This will place demands on the audit department. In particular, it will have to:

- Obtain and nurture audit committee and senior management support for the concept and implementation of continuous auditing.
- Develop and maintain the technical competencies and enabling technology necessary to access, manipulate, and analyze the data contained in disparate information systems.
- Use (or implement) data analysis techniques to support audit projects, including the use of appropriate analytic software tools and development and maintenance of data analysis techniques and expertise within the audit team.

- Sponsor, promote, and encourage the adoption and support of continuous monitoring by management.
- Ensure that continuous auditing is adopted as part of an integrated, consistent approach to risk oriented audit planning.
- Manage and respond to the results of continuous auditing, determining appropriate use, follow-up, and reporting mechanisms. The CAE will have to ensure that appropriate action is taken on the audit findings reported to management and that the results of continuous auditing are considered by management when assessing activities, such as the monitoring of controls, performance measurement, and enterprise risk management.

This IIA Global Technology Audit Guide (GTAG) identifies what must be done to make effective use of technology in support of continuous auditing and highlights areas that require further attention. By reading and following the steps described, internal auditors should be in a much better position to use technology and maximize their return on investment as well as to demonstrate to management the need to make appropriate technology investments — while contributing to compliance with the regulatory requirements impacting their organization and to its overall health and competitiveness.

This GTAG will focus on the technology-enabled aspects of continuous auditing and will address:

- A history and background of similar concepts used during the last 30 years.
- A definition of related terms and techniques: continuous auditing, continuous risk assessment, continuous control assessment, continuous monitoring, and assurance.
- The role of continuous auditing in relation to continuous monitoring.
- Areas where continuous auditing can be applied by the internal audit activity.
- Challenges and opportunities related to continuous auditing.
- The implications for internal auditing and the CAE and for management.
- A continuous auditing self-assessment tool (Appendix C, page 30).

Since 1980, many terms have been associated with the notion of providing ongoing audit procedures in real time or near real time, including: continuous monitoring, continuous control assessment, and continuous auditing. This GTAG categorizes previous approaches under the unifying concept of “continuous auditing.” It discusses continuous control assessment and continuous risk assessment as the main components of continuous auditing. This guide also deems monitoring activities to be management’s responsibility, but discusses the interrelationship between auditing and monitoring and how internal auditors provide additional assurance to support management in their role.

One of the current and most visible drivers for continuous auditing is the high cost of regulatory compliance. In the United States, a Financial Executives International survey (March 2005)² pegged the cost of Sarbanes-Oxley compliance at an average of more than \$4 million per organization. Since most of these costs were related to manual, people-intensive processes — based on use of internal resources and external consultants — it is no surprise that an AMR Research study (January 2005)³ found that key technologies can be used to reduce compliance costs by upwards of 25 percent.

The burden of compliance is pressuring organizations to improve their methods of performing ongoing evaluation of internal controls. In this context, the U.S. Securities and Exchange Commission stated, “both management and auditors must bring reasoned judgment, and a top-down, risk-based approach to the [Sarbanes-Oxley Section 404] compliance processes.” This has led to an increased focus on both continuous monitoring (by management) and continuous auditing. Supporting a comprehensive set of audit activities, continuous auditing not only helps support the audit activity’s assurance of controls, but also risk assessment; the

identification of fraud; waste, and abuse; audit planning; and the tracking of audit recommendations.

Continuous Auditing: A Brief History

The origins of automated control testing began in the 1960s with the installation and implementation of embedded audit modules (EAMs). However, these modules were difficult to build and maintain, and were used in relatively few organizations. By the late 1970s, auditors began moving away from this approach. In the 1980s, early adopters within the audit profession began using computer-assisted audit tools and techniques (CAATTs) for ad hoc investigation and analyses. Coincident with this, the notion of continuous monitoring was first introduced to auditors in a largely academic context. The basic premise was that use of ongoing automated data analysis would help auditors identify the areas of greatest risk, as a precursor to determining their audit plans. For the most part, however, auditors were not ready for this type of approach. They lacked easy access to appropriate software tools, the technical resources and expertise to overcome data access challenges, and most importantly, the organizational will to embrace this new commitment to a significantly different audit approach and methodology.

During the 1990s, within the global audit profession, there was increasingly widespread adoption of data analytics solutions, which were viewed as a critical tool to support the testing of the effectiveness of internal controls. This technology was used to examine transactions for indications of events that occurred because a control did not exist or failed to perform properly. It also identified transactions that did not meet control standards. In addition, data analysis supported the testing of controls not directly evidenced by transactional data. For example, enterprise resource planning (ERP) access and authorization tables could be analyzed to identify failures to maintain appropriate segregation of duties. However, even with this technology underpinning, traditional audit processes often relied on representative samples, rather than assessing the entire population, with analyses continuing to take place some time after the completion of the business activity (transaction). As a result, risk and control problems had a greater opportunity to escalate and impact business performance negatively.

Today’s Audit Environment

Today, proliferation of information systems in the business environment gives auditors easier access to more relevant information — but also involves the management and review of vastly increased volumes of data and transactions.

Further, the rapid pace of business requires prompt identification of, and response to, control issues. Regulations such as Section 404 of Sarbanes-Oxley in the United States require the timely disclosure of control deficiencies and management assertions around the adequacy of the control

² Survey on SOX Section 404 Implementation, Financial Executives International, March 2005.

³ SOX Decisions for 2005: Step Up Technology Investments, John Hagerty, AMR Research, January 2005.

GTAG — Introduction — 2

framework. This statutory compliance imperative, as well as ongoing changes in auditing standards and the evolution of audit software, are encouraging and enabling auditors to adopt new approaches to assessing information and controls.

The CAE must be able to provide senior management with ongoing assessments — rather than simply periodic reviews — of the health of internal controls and levels of risk within an organization. Today's internal auditors do not just audit control activities; they also keep an eye on a company's risk profile and play a key role in identifying areas to improve risk management processes. However, if they do not have a thorough understanding of the business processes and associated risks, auditors can only perform traditional audit checklist tasks. Continuous auditing provides auditors with an opportunity to go beyond the confines of traditional audit approaches and the limitations of sampling, review of standard reports, and point-in-time assessments. A crucial component of continuous auditing is the development of a model for the ongoing (continuous) review of transactions at, or close to, the point at which they occur.

As will be discussed in more detail in Section 4, a key issue that impacts internal auditors' approach to continuous auditing is the extent to which management has implemented systems to monitor controls continuously and identify control deficiencies and indicators of risk.

Continuous auditing measures specific attributes that, if certain parameters are met, will trigger auditor-initiated actions. Under the umbrella of continuous auditing, there are two main activities:

- Continuous control assessment — to focus audit attention as early as possible on control deficiencies.
- Continuous risk assessment — to highlight processes or systems that are experiencing higher than expected levels of risk.

The frequency of the continuous auditing activity will depend on the inherent risk within the process or system. In addition, it is possible to start by examining the key controls and areas of risk, and expand the continuous auditing application as auditors gain experience and achieve measurable results that contribute to compliance, operational efficiency and effectiveness, and financial reporting integrity.

COSO Enterprise Risk Management (ERM) Framework

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Enterprise Risk Management – Integrated Framework* encourages internal auditors to approach their activities from the way management runs a business: control environment, risk assessment, information and communication, and risk monitoring. The COSO ERM framework is an expansion of the original COSO internal control framework. It increases the focus on internal controls and provides a more robust and extensive discussion on the broader subject of ERM. Its four categories



COSO Enterprise Risk Management (ERM) Framework

of objectives — strategic, operations, reporting, and compliance — put pressure on internal auditors to evaluate the internal control system and to identify and assess risk. To do this, internal auditing must change its traditional role to one that focuses on corporate goals, strategies, risk management and business processes, as well as critical control activities.

The focus of continuous auditing is not simply on compliance with controls and regulations, but the improved efficiency of operations in the organization. Continuous auditing also should contribute to the overall improvement of the organization by identifying and assessing risk and providing information to management in order to better respond to changing business conditions. It will help internal auditing in all the COSO ERM components:

- Internal environment and objective setting – by formalizing the objectives of continual auditing and the role of internal auditing.
- Event identification – by developing a system to identify and report on events and a process for dealing with these threats and opportunities.
- Risk assessment – by analyzing and assessing risk, considering likelihood and impact, to form a basis for determining how risk should be managed.
- Risk response – by taking into consideration the risk categories and key activities, and by developing data-driven methodology to assess and respond to risks.
- Control activities – by recognizing the roles of management and internal auditors; demonstrating that control assessment is not a once-a-year activity, but an ongoing concern; and automating the process of testing controls in as near real time as possible.
- Information and communication – by helping to

GTAG — Introduction — 2

ensure the accuracy of information and the timely reporting of concerns.

- Monitoring and review – by providing an independent assessment to support the monitoring activities performed by management.

Continuous control assessment will allow internal auditors to assess the adequacy of management monitoring activities and provide the audit committee and senior management with independent assurance that the controls are working effectively and that the organization can respond quickly to correct deficiencies that arise. Continuous risk assessment enables auditors to identify emerging areas that place the company at risk, prioritize such risks, and 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.

Monitoring and review is the final COSO ERM component of an effective control framework and is a key ingredient in an organization's effort toward continuous improvement. Continuous monitoring encompasses the processes that management puts in place to ensure that the policies, procedures, and business processes are operating effectively. It addresses management's responsibility to assess the adequacy and effectiveness of controls. This involves identifying the control objectives and assurance assertions and establishing automated tests to highlight transactions that fail to comply with the relevant control objectives and assurance assertions. Many of the techniques of continuous monitoring of controls by management are similar to those that may be performed in continuous auditing by the internal audit department.

The Roles of the Internal Audit Activity and Management

In carrying out its stewardship role, management has the primary responsibility for assessing risk and for the design, implementation, and ongoing maintenance of controls within an organization. The internal audit activity, in light of its responsibilities to management and the board, is responsible for identifying and evaluating the effectiveness of the organization's risk management system (IIA Standard 2110) and controls (IIA Standard 2120) as implemented by management. The difference between the roles of auditors and management in addressing internal controls and risk lies in the nature of the respective responsibilities to stakeholders. Auditors conduct the evaluation to provide assurance to stakeholders, the audit committee, and senior management regarding the state of risk and control systems and, in the case of legislation such as Sarbanes-Oxley, the reliability of management's representation concerning the state of controls. Ideally, auditors are not part of the process and do not design or maintain the controls — thereby, retaining their objectivity and independence.

Benefits of Continuous Auditing and Monitoring

The outcomes of continuous auditing and monitoring (by management) are similar and involve notifications or alerts indicating control deficiencies or higher risk levels. The notifications or alerts can be prioritized and, depending on the seriousness of the risk or control deficiency, distributed to the assurers of the business process or application system, operational management, auditors, senior financial management, and even the regulators. Management's response to these notifications can be to rectify a control deficiency and correct an erroneous transaction immediately. The audit response to these warnings may range from an immediate audit of the identified control system to flagging an area for a future audit.

For example, the continuous audit testing of financial transactions may provide notification when a journal voucher is over a given limit and involves entries among an unusual combination of accounts. The auditor's response may depend on whether or not this is seen as a single item — where the response may be to send an e-mail to the originator of the transaction asking for an explanation — or a systemic problem — where a financial audit of the area may be in order. Using continuous auditing, additional tests to determine the nature of the anomaly could answer questions such as:

- Is the journal voucher creating an entry in a suspense account and not being cleared within an acceptable timeframe?
- Is the journal voucher creating entries among unusual combinations of accounts?
- Are the accounts affected likely to be ones that could, for example, artificially inflate earnings?
- Are the volumes and types of journal vouchers unusual compared to previous years?
- Are the individuals creating the entries in a position of compromised segregation of duties?
- Should we tighten or loosen the criteria for this test?
- Are the financial ratios in-line with the company's peers?
- What has been the trend of earnings in recent years, and how does this trend compare with the company's peers and the general economic environment?

Continuous auditing helps auditors to evaluate the adequacy of management's monitoring function. This allows the CAE to provide the audit committee and senior management with independent assurance that control systems are working effectively and that audit processes are in place to identify and address any violations. Continuous auditing also identifies and assesses areas of risk, and provides information to auditors that can be communicated to management to support its efforts to mitigate the risk. Additionally, it can be used when developing the annual audit plan by focusing audit attention and resources on areas of higher risk.

However, one of the greatest advantages of continuous auditing is its independence from both the underlying

GTAG — Introduction — 2

operational and financial systems and the monitoring performed by management. This improves the organization's management and control frameworks and provides mechanisms that auditors can use to support their own independent review and assessment activities.

Continuous auditing is not without its challenges. The technology needs to be understood and controlled. Internal auditors must have access to the data, software tools, and techniques, and have the knowledge necessary to make intelligent use of the vast amounts of corporate financial and nonfinancial information at their fingertips. The opportunities afforded by continuous auditing also place certain demands on auditors and the CAE.

GTAG — Key Concepts and Terms: The Need for Clarity — 3

Various attempts have been made to encourage auditors to make better use of electronic information and to improve the efficiency and effectiveness of the internal audit activity. More recently, a variety of terms have been applied to these initiatives, and the result has created confusion within the profession. Without a clear and common understanding of the terminology, it will be difficult to promote these initiatives, and the likelihood of success will decrease. Therefore, one of the first requirements in the implementation of continuous auditing is the development and dissemination of clear definitions for all related terms.

Key to understanding the terminology surrounding continuous auditing is an understanding of the fact that **control** and **risk** represent opposite sides of the same coin. Controls exist to help mitigate risk; identification of control deficiencies highlights areas of potential risk. Conversely, by examining risk, auditors can identify areas where controls are needed and/or are not working.

Although the assessment of controls and risks always involves both qualitative and quantitative analysis, the greatest gains in efficiency can be achieved by maximizing the use of technology. The challenge to auditors is ensuring the availability and utility of the data, understanding the underlying business processes and systems, and maximizing the use of automation. For this reason, the focus of this GTAG is on the technology-assisted processes that support continuous auditing.

Assurance can be considered to be an opinion to a third party regarding the state of affairs — about a specific transaction, business or governance process, risk, or overall financial performance of a business operation. Audit assurance is a statement regarding the adequacy and effectiveness of controls and the integrity of information.

The **continuous monitoring of controls** by management is at the core of effective assurance strategies; however, auditors must still ensure that management's activities are adequate and effective. The continuous assurance framework is the combination of the activities performed by the internal audit activity to independently evaluate: the state of the controls, risk management within the organization, and assessment of the adequacy of the management monitoring function.



The CAE will need to ensure that all auditors, senior management, and the audit committee understand the roles and responsibilities of the internal audit activity and management in making the continuous assurance equation effective. The following definitions may provide additional insight:

- **Continuous Auditing** is any method used by auditors to perform audit-related activities on a more continuous or continual basis. It is the continuum of activities ranging from continuous control assessment to **continuous risk assessment** — all activities on the control-risk continuum. Technology plays a key role in automating the identification of exceptions and/or anomalies, analysis of patterns within the digits of key numeric fields, analysis of trends, detailed transaction analysis against cut-offs and thresholds, testing of controls, and the comparison of the process or system over time and/or against other similar entities.
- **Continuous Control Assessment** refers to the activities used by auditors for the provision of controls-related assurance. Through continuous control assessment, auditors provide assurance to the audit committee and senior management as to whether or not controls are working properly by identifying control weaknesses and violations. Individual transactions are monitored against a set of control rules to provide assurance on the system of internal controls and to highlight exceptions. A well-defined set of control rules provides an early warning when the controls over a process or system are not working as intended or have been compromised.

The extent to which the internal audit activity is required to perform continuous control assessment activities will depend upon the degree to which management is performing its responsibilities regarding continuous monitoring. A strong management monitoring system will decrease the amount of detailed testing that auditors must perform to provide assurance on the controls.

- **Continuous Risk Assessment** refers to the activities used by auditors to identify and assess the levels of risk. Continuous risk assessment identifies and assesses risks by examining trends and comparisons — within a single process or system, as compared to its own past performance, and against other processes or systems operating within the enterprise. For example, product line performance would be compared to previous year results, as well as assessed in context of one plant's performance versus all others. Such comparisons provide early warning that a particular process or system (audit entity) has a higher level of risk than in previous years or than other entities. The audit response will vary depending on the nature and level of risk. Continuous risk assessment can be used in a large-scope audit to select locations to be visited, to identify specific audits or entities to be included in the annual audit plan, or to trigger an immediate audit of an entity where the risk has increased significantly without an adequate explanation. It also can be used to assess management's actions, to see if audit recommendations have been implemented properly and are reducing the level of business risk.

GTAG – Key Concepts and Terms: The Need for Clarity – 3

- **Continuous Monitoring** is a process that management puts in place to ensure that its policies, procedures, and business processes are operating effectively. Management identifies critical control points and implements automated tests to determine if these controls are working properly. The continuous monitoring process typically involves the automated testing of all transactions and system activities, within a given business process area, against a suite of controls rules. The monitoring typically is put in place on a daily, weekly, or monthly basis, depending on the nature of the underlying business cycle. Depending on the specific control rule and the related test and threshold parameters, certain transactions are flagged as control exceptions and management is notified. The management monitoring function may also be tied to key performance indicators (KPIs) and other performance measurement activities. It is management’s responsibility to respond to the monitoring alerts and notifications and to remediate any control deficiencies and correct defective transactions.

Continuum of Continuous Auditing

Continuous auditing helps auditors to identify and assess risk, as well as establish intelligent and dynamic thresholds that respond to changes in the organization. It also supports risk identification and assessment for the entire audit universe, contributing to the development of the annual audit plan, as well as the objectives of a specific audit. As such, continuous auditing can be seen as a continuum operating on many levels. Also, different points on the continuum are better suited to different tasks, and it is possible to be at more than one point on the continuum as you perform different tasks.

The focus of continuous auditing ranges from controls-based to risk-based (see diagram below); analysis techniques range from the real-time review of detailed transactions to the analysis of trends and comparison of entities against other entities and over time.

- At the “controls” end of the continuum, related audit activities include control assurance and financial attest audits.
- As you move to the other end of the continuum, audit activities include the identification of fraud, waste, and abuse through to the assessment of risk to support audit projects and to produce the annual audit plan.
- Related management activities include continuous controls monitoring, performance monitoring, balanced scorecard, total quality management, and ERM.

Continuous auditing is a unifying structure or framework that brings control assurance, risk assessment, audit planning, digital analysis, and the other audit tools, techniques, and technologies together. It supports micro-audit issues, such as detailed transaction testing to assess the effectiveness of controls, and macro-audit issues, such as using risk identification and assessment to prepare the annual audit plan. It also addresses the mid-level requirements, such as the development of audit objectives for individual auditing.

The main difference between the micro- and macro-audit levels is the granularity of the information required:

- Control testing requires detailed information — down to transactions at the source level. Continuous control assessment uses carefully developed rules and real-time, or near real-time, testing of transactions for compliance with these rules.
- Individual auditing often starts with the risks identified in the annual audit plan but uses more detailed data analysis and other techniques (e.g. interviews, control self-assessments, walkthroughs, questionnaires, etc.) to further define the main areas of risk and focus the risk assessment and subsequent audit activities.
- The annual audit plan requires high-level information — perhaps several years’ worth of data — to establish the risk factors, prioritize risks, and set the initial timing and objectives for the planned set of audits.

← Continuous Auditing →						
Continuous Controls Assessment			Continuous Risk Assessment			Approach
Control-based (Assurance controls are working) Financial Controls			Risk-based (Identification/Assessment of risk) Financial/Operational Controls			Focus
Real-time/Detailed transaction testing (Financial data)			Trend/Comparison (Financial/Operational data)			Analysis Techniques
Control Assurance	Financial Attest	Fraud/Waste/Abuse	Audit Scope and Objectives	Follow-up on Audit Recs	Annual Audit Plan	Related Audit Activities
Control Monitoring	Performance Monitoring	Balanced Scorecard	TQM	ERM		Related Management Activities

GTAG — Relationship of Continuous Auditing to Continuous Assurance and Continuous Monitoring — 4

Continuous Assurance

As mentioned above, assurance can be described as an opinion to a third party regarding the state of affairs. It generally involves three parties:

- The person or group that prepares the information.
- The person or group that uses the information to make decisions.
- The objective third party.

Often, assurance is considered to be strictly an audit-related activity, usually financial in nature. However, others, such as those in the legal profession, provide assurance services as well.

Audit assurance is a statement regarding the adequacy and effectiveness of controls and the integrity of information. The continuous monitoring of controls by management is at the core of effective assurance strategies; however, the audit activity must also ensure that management activities are adequate and effective.

Internal auditing provides assurance services by performing objective examinations of evidence for the purpose of providing an independent assessment of risk management strategies and practices, management control frameworks and practices, and information used for decision making and reporting. Continuous assurance can be provided when auditors perform continuous control and risk assessment (i.e. continuous auditing) and evaluate the adequacy of management's continuous monitoring activities.

Auditors examine the activities performed by management, verify that controls are working, recommend changes, and ensure that risk is being managed. If auditors do their job — checking and verifying controls and risk and ensuring management is doing its job of monitoring — then the organization will have a higher level of assurance that controls are working, risks are being managed, and the information used for decision-making has integrity. Management plays a role in the assurance equation by developing, designing, and monitoring controls, and by managing risks.

Continuous Monitoring

Continuous monitoring refers to the processes that management puts in place to ensure that the policies, procedures, and business processes are operating effectively. It typically addresses management's responsibility to assess the adequacy and effectiveness of controls. Many of the techniques management uses to monitor controls continuously are similar to those that may be performed in continuous auditing by internal auditors. The principles of continuous monitoring are simple and include the following:

- Define the control points within a given business process, according to the COSO ERM framework if possible.
- Identify the control objectives and assurance assertions for each control point.
- Establish a series of automated tests that will indicate whether a specific transaction appears to have failed

to comply with all relevant control objectives and assurance assertions.

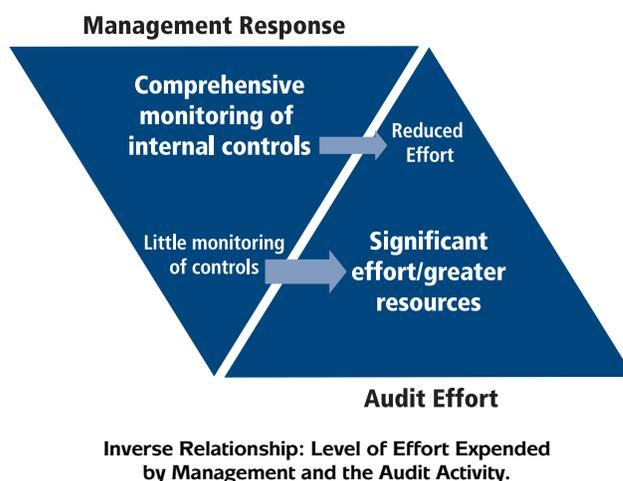
- Subject all transactions to the suite of tests at a point in time close to that at which the transactions occur.
- Investigate any transactions that appear to have failed a control test.
- If appropriate, correct the transaction.
- If appropriate, correct the control weakness.

The key to continuous monitoring is that the process should be owned and performed by management, as part of its responsibility to implement and maintain effective control systems. Since management is responsible for internal controls, it should have a means to determine, on an ongoing basis, whether the controls are operating as designed. By being able to identify and correct control problems on a timely basis, the overall control system can be improved. A typical additional benefit to the organization is that instances of error and fraud are significantly reduced, operational efficiency is enhanced, and bottom-line results are improved through a combination of cost savings and a reduction in overpayments and revenue leakage.

An important additional benefit to the organization is that instances of error and fraud are typically significantly reduced, operational efficiency is increased, and bottom-line results are improved through a combination of cost savings and a reduction in overpayments and revenue leakage.

Continuous Auditing

There is an inverse relationship between the adequacy of management's monitoring and risk management activities and the extent to which auditors must perform detailed testing of controls and assessments of risk. The audit activity's approach to, and amount of, continuous auditing depends on the extent to which management has implemented continuous monitoring.



In areas where management has not implemented continuous monitoring, auditors should apply detailed testing by employing continuous auditing techniques. In some cases,

GTAG – Relationship of Continuous Auditing to Continuous Assurance and Continuous Monitoring – 4

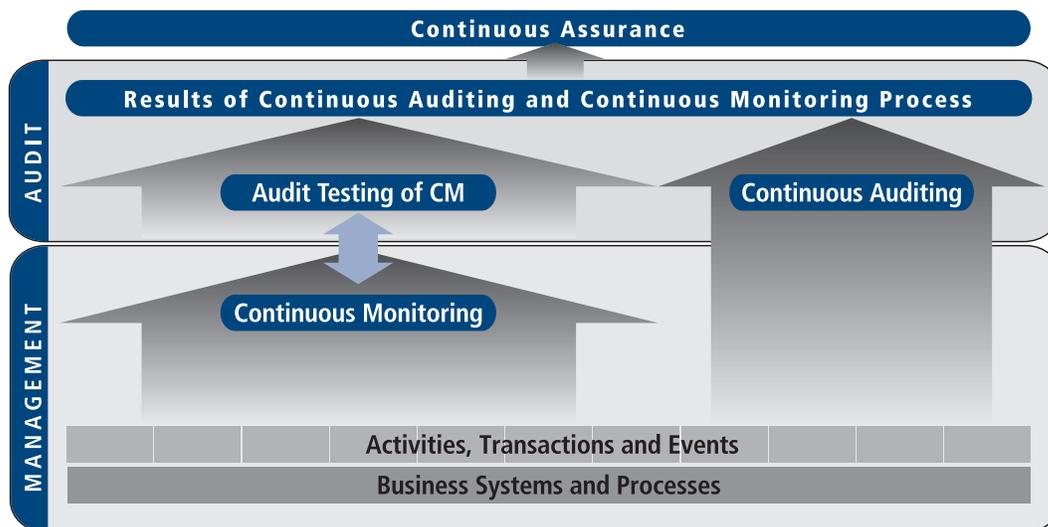
auditors may even perform a proactive role in assisting the organization by establishing risk management and control assessment processes (see IIA Practice Advisory 2100-4: The Internal Auditor’s Role in Organizations Without a Risk Management Process). However, care should be taken to ensure that the auditors do not assume an ownership role over these processes, which may compromise their independence or objectivity.

Where management performs continuous monitoring on a comprehensive basis across end-to-end business process areas, the internal audit activity no longer needs to perform the same detailed techniques that would otherwise be applied under continuous auditing. Instead, auditors should perform other procedures to determine whether they can rely on the continuous monitoring process. Such procedures include:

- Review of anomalies detected and management’s response.
- Review and test of controls over the continuous monitoring process itself, such as:
 - Processing logs/audit trails.
 - Control total reconciliations.
 - Changes to system test parameters.

In general, these procedures are similar to those quality control tests performed during the normal audit process to ensure that computer assisted audit techniques (CAATs) have been applied correctly.

By assessing the combined results of the continuous monitoring and auditing processes, auditors are able to provide continuous assurance regarding the effectiveness of internal controls.



Continuous Auditing, Monitoring, and Assurance (Conceptual Model)

The pressure on internal audit departments to do more with less is increasing. Perhaps the most difficult challenges are for auditors to provide timely assurance on the effectiveness of internal controls, to better identify and assess levels of risk, and to highlight noncompliance with regulations and policies quickly. These are all areas where continuous auditing can be applied. Enabling technologies can range from spreadsheet software or scripts developed using audit-specific software, to commercial packaged solutions or custom-developed systems. The selected solution should be flexible and scalable, allowing auditors to start in one specific area and then to increase scope, scale, and frequency of analysis.

Although some statutory audits are required on an annual basis, the notion of performing audits strictly on an annual basis no longer meets management and regulatory requirements. The internal audit activity must apply risk assessments and perform control assurance activities on an ongoing basis. While regulatory requirements have placed increased attention on the financial aspects of auditing, continuous auditing supports all types and areas of audit activity. The European Confederation of Institutes of Internal Audit (ECIIA), in a 2005 position paper, *Internal Auditing in Europe*⁴, encourages internal auditors to respond to risks facing an organization by providing assurance to management that the risks have been identified and are being managed properly. Auditors must be able to review and assess not only financial, but also operational and strategic risks. This is an emerging area of focus for continuous auditing. The information access technologies and technical skills used to test controls can also help the CAE provide invaluable assistance to management, by supporting evaluation of the ongoing effectiveness of ERM activities and recommending improvements where warranted.

The CAE supports the monitoring function by providing senior management with independent assessments of risks and controls. 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 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.

The CAE should recognize that there are a number of management initiatives with strong links to continuous auditing, such as integrated risk management, balanced

scorecard, continuous improvement, and continuous monitoring. Audit must determine where continuous auditing fits and how it can be used to assess these management initiatives or utilize information generated by them.

The expected benefits of implementing a continuous auditing framework include:

- Increased ability to mitigate risks.
- Reductions in the cost of assessing internal controls.
- Increased confidence in financial results.
- Improvements to financial operations.
- Reductions in financial errors and the potential for fraud.

Further, organizations that have fully embraced continuous auditing typically report reduced operating costs and improved profit margins.

Applications for Continuous Control Assessment

Identification of Control Deficiencies

As new regulations requiring senior management to document and attest to the effectiveness of the control environment and the accuracy of the information contained in financial reports are enacted, chief executive officers and chief financial officers are turning to the internal audit activity to assist in complying with these regulations. Although it is generally accepted that management is responsible for monitoring, designing, and maintaining controls, IIA Standard 2120.A1 states the internal audit activity “should assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvements”. As a result of these external and internal pressures, especially in cases where management is not proactively fulfilling its monitoring role, auditors are often expected to do a more thorough assessment and provide more continuous control assessment. This is having a dramatic impact on internal audit processes and methodologies.

Continuous control assessment provides the CAE with clear insights into the effectiveness of the internal control systems. This, in turn, provides financial executives, business process managers, and risk and compliance officers with independent and timely assurance over internal controls. Continuous control assessment of transactional data against internal controls can rapidly highlight errors and anomalies, reporting them to management for immediate review and action. It can also contribute to the reliability and integrity of financial and operational information, and to the efficiency and effectiveness of operations.

Continuous control assessment also can contribute to the ongoing assessment of risk and management’s mitigation activities. The assessments of controls and risk are complementary activities, each supporting the other.

The following discussion describes example scenarios where the internal audit activity employed continuous control assessments to supplement the management monitor-

⁴ *Internal Auditing in Europe*, ECIIA, February 2005.

ing function in three areas: financial controls, system controls, and security controls.

Financial Controls: Example – Purchasing Card Programs

A national purchasing card manager manually reviewed a small sample of transactions every quarter. The auditors determined that management's controls over what was purchased were weak and the potential exposure to risk was fairly high. After reviewing the applicable policies for purchasing card use, the auditors developed a series of analytic tests to identify:

- Inappropriate card use, including transactions related to travel expenses.
- Purchase of personal items (e.g. jewelry, alcohol, etc.).
- Suspicious transactions (e.g. unauthorized cardholder use, double swiping by merchant, split purchases to avoid financial limits, etc.).

Results of the analyses were forwarded to the managers of the individual cardholders to perform a detailed review of the questionable purchases — matching purchase card receipts to goods purchased. This identified numerous inappropriate purchases and three cases of fraud.

After the audit was completed, the continuous control assessment application tests were turned over to the purchasing card coordinator to assist operational management in monitoring card controls on a monthly basis.

System Controls: Example – Segregation of Duties

Continuous control assessment tests also can be run to verify that system controls are functioning as intended. Using analytic technology, tests can compare individual transactions to rules-based criteria, reviewing all transactions to ensure individuals are not performing incompatible duties.

Within one organization, the implementation of a new enterprise resource planning (ERP) system was intended to replace manual controls with automated controls to ensure appropriate segregation of duties. The ERP programming team, with input from the business owners, developed a series of role-based user profiles that set permissions for the various types of transactions each user could execute based on his or her job function. Although the auditors were satisfied with the approach and the processes involved in developing the role-based profiles, they had concerns about the actual assignment of profiles to users and performed a detailed review of transactions, looking for instances where segregation of duties had not been maintained.

The auditors obtained an extract of all transactions processed in the first quarter of the year and used data analytic technology to calculate the number of transactions processed by each user — by transaction type. This identified two users who had first created purchase orders and then recorded goods receipt transactions for the same purchase orders. The results indicated a weakness in control over segregation of duties in the design of the roles-based profiles, as these were deemed to be incompatible duties.

As the ERP system undergoes additional changes — for example, addition of new roles or changes to existing roles — the continuous control assessment tests are run to verify that there are no cases where segregation of duties has been violated.

Security Controls: Example – System Access Logs

Continuous control assessment can test security controls, verifying that all system users are valid employees and that attempts are not being made to hack into the system.

In another organizational scenario, each week, an extract of the system access log file is sent to the internal audit department. The auditors extract the sign-on information and match each user with a current employee master file. All users who are not employees are flagged, and an e-mail is automatically sent to the system security officer to have the user identifications (IDs) revoked. In addition, the test looks for failed logons. This identified an instance at 3 a.m. where a user ID had 25 failed logon attempts through a dialup connection. The auditors used this report to justify changing the logon parameters such that user IDs were locked after three failed logon attempts.

The potential uses of continuous control assessment are virtually unlimited. Wherever there is an exposure, internal auditors can develop a test or series of analytics to search for evidence of persons trying to take advantage of control gaps or weaknesses. In some cases, the control exposures include potential fraud, waste, and abuse. The frequency and the timing of these tests will depend on the potential business risk and the adequacy of the control framework and management's monitoring function.

Fraud, Waste, and Abuse

IIA Standard 1210.A2 calls for auditors to have sufficient knowledge of the indicators of fraud. Standard 1210.A3 also requires auditors to have knowledge of key information technology risks, controls, and the available technology-based techniques to perform their work. The use of technologies that support continuous control assessment can assist auditors in examining detailed transactions, as well as summarized data, to identify anomalies and other indicators of fraud, waste, and abuse. For example, leveraging data analysis technologies, auditors can easily identify instances where contracting authority was exceeded (i.e. contracts over the contracting limit for the individual) or avoided (e.g. split contracts). In the payroll area, it can be used to identify persons on the payroll who are not in the employee database or to identify unusual rates of pay.

Because fraud is often largely a crime of opportunity, control gaps and weaknesses must be found and, if possible, eliminated or reduced. Widely distributed audit guides and standards address such exposure concerns directly. For example, IIA Practice Advisory 1210.A2-1: Identification of Fraud/1210.A2-2: Responsibility for Fraud Detection requires auditors to have sufficient knowledge of possible frauds to be

able to identify their symptoms. Auditors must be aware of what can go wrong, how it can go wrong, and who could be involved. The American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards (SAS) No. 99, “Consideration of Fraud in a Financial Statement Audit,” was also developed to assist auditors in the detection of fraud. It goes further than its predecessor, SAS No. 82, to incorporate new provisions that include:

- Brainstorming for the risks of fraud.
- Emphasizing increased professional skepticism.
- Ensuring managers are aware of fraud.
- Using a variety of analytic tests.
- Detecting cases where management overrides controls.

It also defines risk factors for fraudulent financial reporting and theft and can be used as a basic model for assessing the risk of fraudulent financial reporting. The risks outlined in SAS No. 99 include factors such as management conditions, the competitive and business environment, and operational and financial stability.

Conclusions and Recommendations

Continuous control assessment techniques may be similar to those used by management in performing continuous monitoring. Where internal auditors can rely on management performance of continuous monitoring, the same level of detailed continuous control assessment techniques is not required. Instead, auditors can focus on performing other procedures to provide ongoing assurance regarding management’s continuous monitoring processes. However, when management monitoring is not sufficient, auditors should perform detailed testing by employing continuous control assessment techniques to evaluate the adequacy of the controls. Through intelligent technology-enabled analytics, auditors can assess the adequacy of the internal control framework and provide independent assurance to the audit committee and senior management.

Continuous control assessments need not be run in real-time. The frequency of analysis will depend on the level of risk and the degree to which management is monitoring the controls. For example, the purchase card analytics may only be run once a month — upon receipt of the purchase card transactions from the credit card company. Payroll may be run every pay period, just before the checks are cut. Tests for duplicate invoices and payments may be run every day. In some cases, an auditor may perform the initial control testing and hand over the ongoing monitoring to management.

Additional practical examples for application of continuous control assessments include:

- Examining transactional data — e.g. flagging all purchase card expenses that are greater than the card limit or that involve prohibited merchants.
- Reviewing summarized data — e.g. total cardholder expenses for the month greater than \$10,000 and where the cardholder is not within the purchasing division.

- Employing comparative analysis — e.g. total overtime payments compared to all other employees in the same job classification and level, to identify potential abuses of overtime (excessive, unauthorized, and so on).
- Testing totals by general ledger account — e.g. highlighting accounts where the amount differs by more than 25 percent compared to the previous year, to identify unusual activity such as an increase in write-offs.

In all cases, auditors can drill down into the details quickly to discover the cause and perform the required follow-up quickly and easily.

Applications for Continuous Risk Assessment

While management has responsibility to develop and maintain a system to identify and mitigate risk, IIA Standard 2110 states that auditors should assist the organization by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems. IIA Standard 2010 encourages the CAE to establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization’s goals. These two activities are related, and auditors can use continuous risk assessment to identify and assess changing levels of risk. This allows them to assess management’s risk mitigation activities and supports the development of objectives for individual auditing and the annual audit plan.

Continuous risk assessment can be used to identify and assess risk on an ongoing basis. It does this by not only measuring transactions against a cut-off, but also by using comparative analysis on the totality of the transactions. Through this type of comparison, auditors can examine the consistency of a process by measuring the variability of a number of dimensions. In operations, for example, measuring the variability in the number of defects is a method for testing the consistency of a production line. The more variability in the number of defects, the more concerns about the proper and consistent functioning of the production line. This same premise can just as easily be applied to the measurement of the integrity of a financial system by measuring the variability (e.g. number and dollar value of the adjusting entries) over time and in comparison to other similar entities. The concept of variability is the key differentiating factor in continuous risk assessment versus embedded audit modules and exception reporting.

By performing continuous risk assessments, CAEs can apply a more strategic context to the development of audit plans and make ongoing adjustments when risk profiles change to keep the audit plan current throughout the year and to allocate scarce, highly skilled audit resources to areas that represent the greatest risk exposure for the organization. Continuous risk assessments can also highlight areas where there are either no controls or the controls are not performing adequately, prompting auditors to perform

continuous control assessments in specific areas. Thus, continuous risk assessment can feed not only the audit plan, but also the continuous control assessment activities.

Example – Risk-based Selection of Audit Sites

With more than 1,100 retail stores located across the country, ABC Food's internal audit department needed an efficient and effective way to select individual store audits. In the past, the auditors tried to visit each store at least once a year to perform a compliance-based audit. However, this was not an efficient means of addressing the real areas of risk.

The CAE needed a reliable risk assessment solution, with data-driven criteria, to be able to provide assurance on all 1,100 stores without having to visit each one every year. Continuous risk assessment was used to establish the necessary analytics, such as reported inventory loss and turnover in experienced staff. Now, the internal audit team can quickly pinpoint stores with the highest degree of risk and develop a more timely, effective, and efficient audit approach.

Development of the Audit Plan

Rather than scheduling audits according to a standard cycle of one-, two-, or three-year rotations, the frequency of audits should be based on the risk factors in a business process. At a high-level, continuous risk assessment supports the development of audit plans, allowing the data-driven identification and assessment of risk indicators. It supports both the establishment of the audit universe and the collection of quantitative data, enabling the internal audit department to focus on the highest risk priorities within the company and to devote appropriate resources to new and changing areas.

The first step is to define the extent of the audit activity's scope and coverage, then to identify measures of materiality and indicators of risk using data from various business systems, such as financial, human resources, and operational information systems. In terms of materiality, one approach is to look at the relative size of each entity — whereas indicators of risk may consider the complexity of the entity relative to other entities. Continuous risk assessment should also include a review of the results of management's monitoring function, including performance measures, quality control, and segregation of duties.

Example – Development of the Audit Plan

The development of a risk-based audit plan at ABC Corp. required the establishment of an audit universe and definitions of audit entities; the collection and analysis of qualitative data such as business plans, organization charts, management input, and facilitated sessions; the collection, normalization, and analysis of quantitative data such as financial, human resources, and operational information; and the prioritization of audits (entities) based on risk indicators.

The following describes how ABC Corp. used continu-

ous risk assessment to support the development of the annual audit plan. Continuous risk assessment was used to measure and prioritize the level of inherent risk related to finance, human resources, and operations for each audit entity.

Financial Measures/Indicators – Financial materiality dealt primarily with the total dollars in expenses, revenues, and assets. This varied considerably; for example, not all of the audit entities had revenue and some had no assets. The complexity indicators considered not only changes compared to the previous year and relative size, but also items such as the number of responsibility centers, percentage of discretionary spending, and whether or not the entity had to manage expenses, revenues, and assets. For example, Entity A, with \$15 million in expenses — mainly salary dollars — would not have the same level of financial risk as Entity B, with \$5 million in expenses (82 percent of which is discretionary), \$10 million in revenue, and \$12 million in assets. Also, if this is the first year Entity B had any revenue, that would raise the level of financial risk.

Human Resources Measures/Indicators – Human resources materiality considered the total number of personnel, whereas the complexity indicator examined the mix of personnel (e.g. employees vs. contractors, full-time vs. part-time) as well as staff turnover and loss of key skills. It also considered changes compared to previous years (e.g. a rapidly growing organization may have different risks than one that is stable) and the number of locations (i.e. geographic dispersion) of the entity.

Operational Measures/Indicators – In ABC Corp., operational measures and indicators were primarily concerned with the number of products; hence, materiality also was tied to the number of products. Complexity was related not only to changes in product number and mix, but also production lead times, responsiveness to customer demands, and the complexity of the manufacturing process. Manufacturing complexity was broken down into three categories — high, medium, and low — based on the length of time involved in the manufacturing process. The notion was that a product with a 20-hour manufacturing process time not only takes longer to produce, but carries a higher level of operational risk than a product with a manufacturing process time of two hours. Manufacturing personnel vetted this assumption as a reasonable proxy for complexity.

Once all of the data from the three business systems was collected, normalized, and analyzed for each audit entity, the relative score was calculated for each entity. The score was determined by counting the number of times an entity was in the top 10 for the given risk indicators. The entities were ranked against all other entities, not to cut-offs. Since an absolute number or cut-off was not used for any attribute, there was no need to adjust parameters as performance improved.

With a rapidly changing business environment, annual audit plans may not be sufficiently responsive to changing levels of risk. However, through technology-assisted activi-

ties, it is easy to update risk assessments and monitor the risk indicators on an ongoing basis. Risk assessment tests can be run frequently to ensure that planned audits address current or emerging risks. In addition, by comparing the results of the risk assessments over time, auditors can anticipate emerging risk exposures before they become serious. The results can be used to set the parameters for the formal audit action and to determine its timing.

The audit response can vary in intensity and urgency based on the level of risk. The early identification of a risk may not require a full audit, but a simple management letter outlining the exposure and requesting a management response. This will not only focus audit resources on areas of greatest risk, but also maximize the effectiveness of these resources.

Support to Individual Auditing

Continuous risk assessment also contributes to individual auditing by supporting the identification and assessment of risk and the development of scope and objectives. Further, it can be used to determine which locations will be visited and identify specific criteria (e.g. lines of inquiry).

The primary difference between the use of continuous risk assessment to develop the enterprisewide annual audit plan and to support individual auditing is the degree to which detailed information is used to identify and assess risk. The enterprisewide audit plan may only require summary-level information for each entity, whereas, on an individual audit level, more detailed information is required to identify risk at a level that supports the definition of the audit scope and the development of audit objectives for a given audit.

In a conventional audit, the scale and scope of analytical review procedures is limited by the type and amount of data that can be collected by traditional techniques. Continuous auditing has the potential to increase the quantity and scope of data available to the auditor. The deployment of continuous auditing methodology provides the opportunity to widen the scope and increase the scale of analytical review procedures dramatically. For example, a yearly reconciliation, once automated, can be programmed into a continuous auditing procedure and performed more frequently. Ratios that are calculated in analytical review can be incorporated into the continuous auditing software, computed on a more frequent basis, and reviewed and compared with critical values. Then, significant variances can be flagged.

Example – Support for an Accounts Payable (AP) Audit
As part of the risk assessment performed during the planning of an audit of the AP function — to be performed at numerous sites across the country — the auditor calculated the volume and cost per transaction processed by AP offices, and the staffing numbers and skills. The overview analysis determined that AP was decentralized with no standard processes. Moreover, different transaction types were being processed at

different offices. In addition, the auditors used “cost per transaction” and “number of transactions per user” to assess the impact of different invoice processing operations, identifying concerns in efficiency and effectiveness at certain offices. The results were used to determine which locations should be visited as part of the on-site work.

In cases where the same audit is performed at several locations or annually, specific audit tests can be performed, and the results can be compared to other entities or over time. Continuous risk assessment can be used to look at specific risks, such as failure to make effective use of purchasing cards. For example, comparing two years’ worth of data for each entity to identify trends provides auditors with a better understanding of which entities are making positive progress. Continuous risk assessment can also be used to assess the impact of any changes in the process by performing the same analysis in subsequent years. Additionally, future years’ data can be added easily to assess the impact of the implementation of the audit recommendations.

Follow-up on Audit Recommendations

By linking data-driven indicators to recommendations, auditors can use continuous risk assessment to determine if recommendations have been implemented and if they are having the desired effect of reducing the level of risk. In particular, if continuous risk assessment was used to identify and assess risk as part of the development of the audit scope and objectives, the same indicators can be used to evaluate the impact of the implementation of the audit recommendations.

Ideally, every audit will identify data-driven indicators for each recommendation. This will make it easy to establish a baseline and compare results — before and after the implementation of the recommendation. However, it means that auditors will need to find appropriate indicators that can be measured electronically. These indicators can be proxies for what is being measured. For example, if an audit determined that employee morale was low, a recommendation could focus on improved communications. The auditor may measure the number of sick days being used or the number of formal complaints reported. Although this doesn’t directly measure morale, the auditor could use these indicators, as they would be responsive to changes in morale. Evidence of a reduction in sick days and reported complaints could be used to show that improved communications were implemented and were having the desired effect.

Example – Purchase Orders

A financial control requires every purchase over \$5,000 to reference a purchase order. The auditors had established a continuous audit test that examined all invoices greater than \$5,000 to validate the required purchase order reference. Initially, it flagged many cases where purchasers were not following the policy. The auditors recommended a change to the edit controls in the financial system. One month later, after the implementation of the new edit check, the test

reported that all transactions over \$5,000 were now referencing a purchase order.

Although the test indicated that the controls were working, the auditor wondered if they were working properly. A quick test was performed to determine the total amount of the invoices that referenced a purchase order and to compare this total to the purchase order amount. Because the deliverables related to a purchase order can be received across several shipments, there were several invoices for some of the purchase orders. The auditor was surprised, however, to find purchase orders with 100 or more invoices and payments totaling hundreds of times the original purchase order amount. The auditor determined that although each invoice over \$5,000 did reference a purchase order, some users were simply using the same purchase order over and over again.

The follow-up on the audit recommendations examined 100 percent of the transactions over \$5,000 and determined that the initial recommendation had ensured a purchase order was referenced, but did not address the problem of invoices not referencing the proper purchase order.

Conclusion

Continuous risk assessment is not a static system. The identification of indicators and assessment of their use and value are key tasks. Internal and external risks must be assessed continually so that risks on the horizon are addressed in a timely manner and the organization responds to the changing risk environment. The CAE should ensure that appropriate notification systems are in place to provide feedback on emerging risks. Risk alters should be prioritized and managed with clear understanding of who receives them, how they are communicated, and what action should be taken. Secondly, auditors must continually receive feedback on the utility of continuous auditing in assessing risk and must develop strategies for improving the process and reporting the results. In particular, the CAE must determine how the audit results will be used in the ERM activity performed by management.

GTAG — Implementing Continuous Auditing — 6

The notion of continuous auditing is not a difficult concept; however, widespread continuous auditing has not been implemented by internal auditors, and senior management has not fully accepted and funded the necessary technology. Successful implementation requires buy-in by all involved and a phased approach that initially addresses the most critical business systems. Although each organization is different, there are a number of common activities that must be planned and managed carefully when developing and supporting the use of continuous auditing (see "Key Steps" below). The sequence of these activities may vary. Additionally, there may be other activities not identified below, particularly when developing continuous auditing to support a specific audit.

Continuous Auditing Objectives

Many organizations have been evaluating the introduction of continuous auditing to support the control assessment requirements of regulations such as Sarbanes-Oxley. Although having an adequate automated system for testing controls contributes to the assessment of internal controls and the overall mandate for a higher standard of corporate governance, additional benefits in the form of improved business performance can be equally significant. It is important for the CAE to consider the short- and long-term objectives of continuous auditing. The effort involved in gaining access to, and knowledge of, the key business systems and processes has the potential to both reduce the burden of compliance and eliminate drags on business performance.

KEY STEPS

CONTINUOUS AUDITING OBJECTIVES

- Define the objectives for continuous auditing.
- Obtain and manage senior management support.
- Ascertain the degree to which management is performing its monitoring role.
- Identify and prioritize areas to be addressed and types of continuous auditing to be performed.
- Identify key information systems and data sources.
- Understand the underlying business processes and application systems.
- Develop relationships with IT management.

DATA ACCESS AND USE

- Select and purchase analysis tools.
- Develop access and analysis capabilities.
- Develop and maintain auditor analysis skills and techniques.
- Assess data integrity and reliability.
- Cleanse and prepare the data.

CONTINUOUS CONTROL ASSESSMENT

- Identify critical control points.
- Define control rules.
- Define exceptions.
- Design technology-assisted approach to test controls and identify deficiencies.

CONTINUOUS RISK ASSESSMENT

- Define entities to be evaluated.
- Identify risk categories.
- Identify data-driven indicators of risk/performance.
- Design analytic tests to measure increased levels of risk.

REPORT AND MANAGE RESULTS

- Prioritize results and determine the frequency of the continuous auditing activities.
- Run the tests on a regular, timely basis.
- Identify control deficiencies or increased levels of risk.
- Prioritize results.
- Initiate appropriate audit response and make results known to management.
- Manage results — tracking, reporting, monitoring, and following-up.
- Evaluate the results of the actions taken.
- Monitor and evaluate the effectiveness of the continuous auditing process — both the analysis (e.g. rules/indicators) and the results achieved — and vary the test parameters as required.
- Insure security over the continuous auditing process and ensure that there are appropriate linkages to management initiatives such as ERM, monitoring, and performance measurement.

GTAG — Implementing Continuous Auditing — 6

Now is the time to move beyond simply commenting on the reliability of the financial reports every quarter to embracing a continuous auditing paradigm that contributes to the overall health of the organization and to its operating efficiency and effectiveness. In particular, the internal audit department needs to address the end-to-end business process (COSO) and IT (Control Objectives for Information and Related Technology, or CoBIT) controls present in virtually every business activity. The reliability of business systems and transactional data is paramount, not only to the internal control framework and the integrity of financial reporting, but also to the efficiency of business operations. Thus, ensuring the reliability, integrity, and availability of business systems and data should be a key objective for the CAE and senior management. Continuous auditing can help the organization achieve this objective by facilitating the assessment of the effectiveness of controls and the levels of risk.

A description of the steps involved in implementing a continuous auditing solution follows.

Define Audit Requirements

To meet emerging audit objectives, CAEs must understand future audit processes and continuous auditing techniques. The requirements must be defined adequately by internal auditors — with input from management and external auditors — which necessitates that auditors understand the industry, organization, business processes, related controls, as well as the use of technology-based solutions. This requires an investment of time, but if continuous auditing is to be used to test controls, identify and assess risk, detect and deter fraud, or to support other audits, the benefits are well worth the effort.

Obtain Management Support

Once the objectives of continuous auditing have been defined, audit committee and senior management support should be obtained. They must not only be aware of the continuous auditing initiative, but must also fully support it. The audit committee and senior management must be informed of the pre-conditions, in particular the access requirements, as well as how and when the results will be reported. If this is not done, when anomalies in transactions are identified and managers are contacted for explanations, the legitimacy of the continuous auditing activity may be questioned. The manager's first question, when contacted for explanations of unusual transactions, may well be, "I was not informed of any approved audit in this area. What audit is this in relation to?" This questioning slows down the process, as the auditor will have to explain the concept and objectives of continuous auditing before dealing with the identified control weakness or risk area.

Determine Scope of Testing

The next step in the process is to determine the extent to which detailed testing of controls and risks must be

performed by the audit activity. A key factor in this determination will be the adequacy of management's actions and monitoring activities. The CAE should examine the control framework and areas addressed by ERM. If management has well established and functioning processes to assess controls and risk, then the audit activity will be able to place more reliance on the control and risk levels being reported. However, if the CAE determines that the processes are not adequate, auditors will, of necessity, be required to perform their own detailed assessments of the controls and risks on a more continual basis.

Identify Information Sources

Once the extent of continuous auditing was been determined, the next step is to identify the information required to address the defined objectives and to determine the possible sources of that information. Although this step is similar to that undertaken for any audit or control review — whether computer assisted or not — auditors should try to avoid being constrained by old modes of thinking. They must have a clear understanding of what they are trying to accomplish before defining the information requirements. Identify what needs to be accomplished, not how it will be done. The "how" will be determined at a later stage.

Negotiate Access to Data

Getting the right data is a critical juncture in the implementation of continuous auditing. The CAE must identify the business applications to which the audit department requires access and determine which of these applications are the most critical. The next step is working with the system owners to negotiate access rights. A good working relationship with IT management is invaluable, as their help is often required, even if auditors are experts in using data analytic tools. Too often, the system documentation for the enterprise, mainframe, or custom-built applications housing the required data sources is lacking or out of date, and the only source of information about the data sets is the IT support personnel.

All auditors must be aware of the importance of identifying electronic sources of information inside and outside of the company. For example, auditors doing fieldwork in branch offices may discover end user-developed applications that could be of use for continuous auditing. Auditors should strive to find, collect, analyze, interpret, and document automated sources of information to support the results. The information collected should be factual, verified to source, relevant, and useful to provide a sound basis for results. In searching for sources of information, auditors should start by assuming that the information exists in electronic form, and where possible:

- Determine the possible sources and application systems.
- Identify the owners of the information. (Auditors may need their permission before IT can grant them access to the application system or the data files.)

GTAG — Implementing Continuous Auditing — 6

- Identify the programmer/system analyst responsible for the application system.
- Obtain all necessary documentation, such as data dictionary, record layout, system overview, and business processes.

Auditors should not be constrained by the first information system they discover. A more vigorous search will often find better or corroborating sources of the information required. The system- and business process-owners can be invaluable in this process. Discussions with data owners and application programmers/analysts can assist auditors in determining the best source of information. These discussions can also serve to identify key fields and other sources of useful data. Always consider both local office and headquarters data sources. Where two sources of data exist, comparisons of the data can prove to be extremely fruitful in identifying control deficiencies and risk exposures.

Understand Business Processes

Once the main data sources have been identified, auditors must understand not only the information systems, but also the supported business processes. A basic understanding can be obtained from the existing documentation as follows:

- Review the general system description documentation, such as user and programmer manuals, system flowcharts, copies of input documents, sample output reports, and descriptions of the system controls.
- Interview system users and programmers.
- Interview business process managers.
- Review existing standard reports and exception reports.

A more in-depth knowledge of the system can be acquired by:

- Analyzing detailed system flowcharts and/or a narrative of the data flows.
- Examining copies of all input and output documents.
- Studying record layouts for all data files, including field descriptions and explanations of possible values for each field.
- Examining transaction counts, exception, and summary reports and comparing these to other reports or systems.

Involving all auditors in the process of identifying possible sources of information can help to change the audit outlook from the traditional looking-at-the-past thinking to a forward-looking view by using continuous auditing as an integral audit tool. The end result of this effort should be a detailed understanding of the key business systems, the controls, and key data elements. In addition, auditors should have secured access rights and be capable of performing extraction, normalization, and analysis of the data.

Identify Key Controls and Risks

The ultimate goal of continuous auditing is to ensure the effectiveness of all controls and support the mitigation of risks. In practice, this can be best achieved by identifying key controls and risk categories. As noted in the U.S. Public Company Accounting Oversight Board (PCAOB) guidance on implementing Auditing Standard No. 2, auditors should use risk assessment to determine which controls should be examined. The CAE should pursue those activities that will provide the most immediate and largest payback. Auditors need to build on success stories that demonstrate the feasibility and utility of continuous auditing. Therefore, the prioritization of business processes and systems predisposed to continuous auditing is required. In setting the objectives, the CAE should also determine the knowledge, skills, and disciplines needed to carry out continuous auditing effectively. In particular, auditors will need the appropriate type and level of technical expertise and access to appropriate, purpose-built technologies.

Data Access and Use

As with any use of technology, continuous auditing is not purely a technical issue; however, the selection of the enabling technology is critical to long-term success. (See *Continuous Auditing: Potential for Internal Auditors*, Chapter 5 – Enabling Technologies, IIARE, 2003, for a list of technologies that will likely play a role in developing continuous auditing methodologies.) A clear set of objectives for continuous auditing and a plan to determine the corresponding risks and priorities will help to guide the software selection. When selecting software for continuous auditing, the CAE should consider the data sources, formats, and transaction volumes. It is also important to examine the company's computing environment and future plans for key business systems. Although more sophisticated continuous auditing applications may be required for longer-term sustainability, there are also options to take advantage of the flexibility of audit-specific analytic software solutions. Audit software can read diverse data types, including mainframe legacy systems, client/server, and Internet-enabled systems, or enterprise resource planning applications like SAP, Oracle, and PeopleSoft. It can easily combine and analyze data from various systems and platforms.

Not surprisingly, continuous auditing requires access to data. Audit departments that have not secured electronic access to their company's data are running out of excuses and, perhaps, out of time. With advancements in technology — both hardware and software — the issue of data access is no longer a major technical hurdle and does not require specialized hardware or the involvement of IT personnel. Often, accessibility challenges stem from management reluctance to provide auditors with access to the organization's application systems. Support from management is often necessary for auditors to obtain physical and logical access to the required information. This may require a statement in the audit char-

GTAG — Implementing Continuous Auditing — 6

ter from senior management such as: “Auditors will be given access to any and all application systems and information required to perform their duties.” Having secured management support for access to systems and information, the auditors must ensure that owners of the data are well informed of their access rights and requirements. The CAE must also ensure that the access and use of business systems’ data does not adversely affect the operational performance of these systems, and that audit technology is compatible with the enterprise IT environment.

Accessing Data

To use continuous auditing effectively — to perform the ongoing analysis and follow-up on results — access to the information in electronic format is necessary. The access method will depend on the objectives set for continuous auditing and should take into account factors such as volumes of data, network traffic, system performance, and so on. The CAE also will need to ensure that proper access rights have been attained. For mainframe and client/server systems, security-cleared read-only access is required.

Continuous auditing usually requires a combination of several of the following access methods:

- Embed the continuous auditing software in the business system to process the data in place.
- Obtain independent access to the system’s data files, not using the application’s software, and extract and prepare the data for use by the continuous auditing software.
- Run copies of standard reports and save reports in electronic format for further analysis.
- Run queries or generate reports with a report writer.
- Obtain physical and logical access to the client system and sign on as a user with read-only access rights.

The combination of access methods used should allow auditors to run the continuous auditing in a timely manner and to identify and report on highlighted transactions. It should also allow auditors to easily identify transactions with similar parameters, and to follow-up on flagged transactions.

Accessing and using data from almost any source requires a good understanding of the record layout. There are several file attributes that are possible when accessing and transferring data. It is important to not only understand the data file structure at the macro-level — for example, a flat file, a delimited file, or a number of relational databases — but also at the field level. A record layout contains information about how the records are structured and which fields are stored in a data file. It is used as a reference when defining the data to the analysis package, providing information on the field names, data types, field lengths, and decimals.

Before continuous auditing can begin, the data file must be accessible by the auditor. This often requires the transfer of the data from the business system to the auditor’s computer. Today, there are many different methods to achieve this

transfer. Discussions with business system owners can help auditors to determine the transfer method and the data file format best suited for continuous auditing.

Build Audit Technical Skills and Knowledge

IIA Standard 1210 requires that internal audit collectively should possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities. The first GTAG, on information technology controls, states that “Varying levels of IT knowledge are needed throughout the organization to provide a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control, and governance processes. Knowledge of how IT is used, the related risks, and the ability to use IT as a resource in the performance of audit work is essential for auditor effectiveness at all levels.”⁵

The Canadian Institute of Chartered Accountants (CICA) and AICPA research report on continuous auditing also notes that a high degree of proficiency in IT and the audited subject matter is essential for all auditors. Thus, the audit department must have properly trained and knowledgeable personnel dedicated, or specifically earmarked, to support continuous auditing. In particular, the auditors developing and maintaining the continuous auditing applications will need to have a strong knowledge of the systems being accessed and the underlying systems and functions generating the transactions being monitored.

In the initial phase, the sensitivity of the parameters, the robustness of the analyses, and other factors may cause a large number of transactions to be flagged by continuous auditing. This should be expected. The workload required to follow up on the results will decrease as controls are improved, analytics are refined, and continuous auditing matures.

The preliminary results of continuous auditing may also be prone to errors in interpretation of the data or the results. This is frequently due a lack of understanding and familiarity with the business systems and the nature of the tests being performed. Auditors must have a sound understanding of the information system and the underlying data supporting it. Understanding the data under examination before reporting the results is critical to successful continuous auditing. Failure to understand what the data represents will invariably lead to false conclusions that fail to identify critical control weaknesses or identify weaknesses where none exist. The time and effort spent developing an understanding of the data (and ensuring its accuracy and completeness) will help auditors render an accurate analysis. This can be achieved by:

- Reviewing the key data fields and data elements.
- Reviewing meta-data created by functions applied to the data.
- Ascertaining the timeliness of the data. (Is the information current? How often is it updated? When was the last update?)

⁵ GTAG *Information Technology Controls*, The IIA, March 2005.

GTAG — Implementing Continuous Auditing — 6

- Determining if the information is complete and accurate.
- Verifying the auditor's assumptions and analysis with the system programmers.
- Verifying the integrity of the data by performing various tests such as reasonability, edit checks, comparison with other sources, including previous investigations or audit reports (e.g. syntactic, semantic, and pragmatic data integrity).

Given that all auditors are a potential source of information concerning local and corporate applications, communication is a critical issue to the understanding of the information sources. The knowledge gained from informal and other channels must also be shared. Audit departments should develop mechanisms, such as Intranet or groupware, to ensure all auditors have access to information systems and the associated documentation.

Ensure Integrity of Data

The integrity of data is very important to the smooth application of continuous auditing techniques. Auditors must ensure the integrity of not only their analysis, but also the data and their interpretation of the results. Initially, auditors will have to perform an assessment of the business systems' data integrity. But, how and to what degree must the integrity be examined? How much is too much (i.e. over-auditing) and when is it not enough (i.e. under-auditing)? The answers to these questions lie in assessing the consequences of relying on faulty results and determining the amount of testing and verification necessary to reduce audit risk to an acceptable level.

Consider Uses of Data

Now that the key business systems have been identified, the data accessed, and integrity verified, auditors should consider how the data would be used. One of the powers of continuous auditing is the ability to extract data from a variety of systems across the organization and to combine this information for further cross-platform analysis. For example, an organization may have a control that states that all purchases over \$5,000 must reference a purchase order. However, the purchasing and invoice payment data are in separate systems. The continuous auditing system could test this control by combining the purchase and invoice payment data to identify invoices for more than \$5,000 that do not have a corresponding purchase order record. The combining of data from disparate systems often requires data cleansing to remove transactions with integrity problems, to modify data formats, and so on. Audit software is particularly well suited for cleansing data from different systems to make it easier to work with. For example, if one system captures employee identification numbers in the format xxx-xxx-xxx and the other has the format xx-xxxx-xxx, audit software can quickly establish a common format.

Continuous Control and Risk Assessment Relationship

A key ingredient of the continuous controls-risk continuum is the free flow of information in both directions. Auditors performing continuous risk assessments should not only feed management's ERM activities, but should also use the results from the risk assessment as input into the continuous controls assessment. IIA Standard 2120.A1 states:

Based on the results of the risk assessment, the internal audit activity should evaluate the adequacy and effectiveness of controls encompassing the organization's governance, operations, and information systems.

Not surprisingly, an increased level of risk could easily point to a deficient or nonexistent control. Conversely, identified control deficiencies should be considered when examining the levels of risk. This does not imply that increased risk demands additional controls or that control weaknesses necessarily produce increased risk. However, the results from an assessment of one should be input into the assessment of the other.



The audit activity and the CAE can add significant value by:

- Reviewing critical control systems and risk management processes.
- Evaluating the effectiveness of management's risk assessments and the internal controls.
- Providing advice concerning the design of — and improvements to — the control framework and risk mitigation strategies.

Continuous Control Assessment

The importance of controls in the financial reporting and operational business processes cannot be overstated. The integrity of business processes relies on controls compliance, effectiveness, and efficiency. Controls must assure the confidentiality, integrity, availability, and reliability of information. Auditors must be increasingly vigilant in providing continuous control assessment to validate that these controls are effective.

Continuous control assessment provides independent analysis of transactional data through pre-designed control tests. Typically, these tests are based on the COSO framework. The use of continuous control assessment permits the

GTAG — Implementing Continuous Auditing — 6

CAE to provide management with an early warning of control violations or deficiencies.

The power of continuous control assessment does not lie in the ability to identify simple exceptions, such as values that exceed a threshold (e.g. purchase card transactions over \$10,000) or instances where required information is blank (e.g. no reference to a purchase order). These are known symptoms, and a continuous control assessment system can easily test for them.

The true power of continuous control assessment lies in the ability to perform more complex and sophisticated tests of controls. These tests can use:

- Detailed transactions (e.g. authorization by a user without sufficient authority for the type of transaction, or payments to a vendor with the same name as the user approving the transaction).
- The totality of the transactions (e.g. invoices more than two standard deviations over the average).

Continuous control assessments can also identify exceptions, which manifest themselves as anomalies. Examples include:

- Vendors with only one invoice in the quarter.
- Higher than expected contracting amount of \$49,000, bypassing controls on contracts over \$50,000 (identified through Benford's Law analysis).
- Instances where a single user processes all contracts with a given vendor and shares the same addresses as that vendor.

Auditors must examine the operational environment and its internal controls to identify where weakness and deficiencies may leave the company exposed to risk. The system of internal controls must be evaluated and tested to ensure it is working as intended. Processes, control points, key players, and risks must be reviewed carefully.

Identification of Control Objectives

But where do you start? The COSO or CoBIT framework can be used to assist with the process. The best place to start is to identify the key controls. Initially, management, with support from the internal audit department, should identify the main business activities and their sub-processes, then determine the related control objectives. The control objectives could be classified under the COSO headings of authorization, accuracy, completeness, validity, efficiency and effectiveness, segregation of duties, and regulatory compliance. For example, the processes surrounding purchase requisitions include create, edit, order goods, and adjustments.

Identification of Key Controls

Continuous control assessment starts with the identification of the controls over the key business processes. Auditors and management need to be concerned with the evaluation of controls for the efficient and effective use of company

resources. Sound controls are an essential part of any defense against fraud, waste, and abuse, but they may not be working as intended or may no longer be adequate. Reorganization, business re-engineering, or downsizing can seriously weaken or eliminate controls, while implementation of new IT systems can present additional opportunities to commit or conceal fraud. They must also be constantly aware that mandated controls nominally in effect might be poorly enforced or otherwise irrelevant.

Definition of Appropriate Control Test Analytics

Once the key business processes, sub-processes, and related control objectives are defined, internal audits should rank them to identify the critical controls points (highest impact/risk). Taking the most serious control points, the next step is to define appropriate analytics for each control objective. A simple question that needs to be answered: "What would the data look like if the control objective was not met?" Tests can then be developed to look for the symptoms of the exposures. For example, given the control objective that requisitions should be authorized properly and comply with stated limits, tests can be developed to look for unauthorized requisitions, requisitions authorized by persons without the proper authority, and requisitions that have been split into two or more pieces to avoid financial limits.

Continuous Risk Assessment

Risk management seeks to align the organization's strategies, processes, technology, and knowledge to improve its ability to evaluate and manage the uncertainties that may impact the ability to accomplish its objectives. As such, risk management is an essential management function. However, IIA Standard 2110 states that audits should assist the organization in identifying and evaluating risk exposures. Standard 2010 also states that the audit department's planned activities should be based on a risk assessment.

Evaluate the ERM Framework

In developing a continuous risk assessment capability, auditors should first determine if management has implemented an ERM function. If ERM is being performed, auditors can start by reviewing the adequacy of the risk management activities performed. If ERM is not being performed properly by the organization, the continuous risk assessment will have to be developed from scratch and must be more robust and performed more frequently by the internal audit activity. A good place to start is COSO's *Enterprise Risk Management – Integrated Framework*.

Understand the Areas of Potential Risk

For auditors to identify and assess the levels of risk, they must understand the mission, key business objectives, and sub-objectives of the organization. In addition, they must know where and what could possibly happen to the organization in the normal course of operating its business, or as the result of

GTAG — Implementing Continuous Auditing — 6

some other unusual event. The CAE must keep abreast of what's happening in the internal and external environment that might impact the ability of the organization to achieve its objectives. Auditors must be aware of not only the areas where their organization could be at risk, but also the potential impacts.

Consider Types of Risk and Consequences

The next step in performing continuous risk assessment is to consider the risk categories or types of exposures. Typical risk categories include:

- External environment
- Legal.
- Regulatory.
- Governance.
- Strategic.
- Operational.
- Information.
- Human resources.
- Financial.
- Technology.

The risk categories can help identify and assess the risks. Risks that are poorly managed or not mitigated represent an exposure to the health of the organization. The identification of the risk categories will help auditors to consider where potential events might affect the achievement of business objectives.

Identify the Consequences of Risk Exposure

The next step is to identify the consequences of risk exposure. Will the risk result in a monetary loss or theft of assets, or a loss of proprietary data or competitive advantage? Still, even if auditors are able to identify all the possible exposures, there likely will be a lack of resources to deal with them all. To focus audit attention effectively, auditors must not only identify and assess risks; they must also understand the risk appetite of the organization and be in a position to prioritize the identified risks.

Assess the Level of Risk

Once the exposures have been identified, it is important to assess the level of risk. Two of the usual measures of risk are likelihood and severity. Likelihood is the measure of the certainty that the exposure will result in a loss. Severity is the extent to which the impact will be felt. The risk assessment should include the examination of the controls in place to mitigate against these risks.

Collect and Analyze the Data

The last step in continuous risk assessment is the collection and analysis of data supporting the key business processes and areas of highest risk. Often, this must be gathered from many levels of the organization to identify, assess, and respond to risks. Business owners and IT professionals can help auditors develop data-driven indicators of risk. These indicators should react to changing levels of risk and be easily measurable.

The results of continuous risk assessment will support the

currency of the audit plan, perhaps resulting in a specific audit to be added to the plan. They also can be useful when developing scope and objectives for an individual audit and can be provided to management for information and attention.

Manage and Report Results

The CAE should consider the objectives of continuous auditing, the risk appetite of the organization, the level and nature of management monitoring, and the enterprise risk activities when setting the timing, scope, and coverage of the continuous auditing tests. In some cases, auditors should prioritize the risks and select only a few high-risk areas or key control points for the first implementation of continuous auditing.

The next step is determining how often the continuous auditing tests will be run. The frequency of continuous auditing activities will range from a real-time or near real-time review of detailed transactions to periodic analysis of detailed transactions, snapshots, or summarized data. The frequency will depend not only on the level of risk associated with the system or process being examined, but also on the adequacy of the monitoring performed by management. Critical systems with key controls may be subject to real-time analysis of transactional data. Continuous auditing tests in payroll may be executed just prior to the payroll run (e.g. every two weeks or twice monthly). Purchase card transaction tests may be run on a monthly basis, when the purchase card data is received from the credit card company. Risk assessments to support the annual audit plan may be conducted quarterly, while those supporting individual auditing and the tracking of audit recommendations may occur daily.

There is no simple answer to how often continuous auditing tests should be run — except perhaps to say that more often is better than less often. An important consideration when discussing frequency is the fact that the automation of continuous auditing tests will lower the cost of performing risk assessments and control verification. Typically, examining 200 invoices manually will take twice as long as examining 100. Fully automated tests are easily scalable (by number and frequency), so that the frequency of operation or volume of transactions considered does not imply additional workload or cost. Since the continuous auditing software performs the analysis, analyzing one million transactions every week is no more work than reviewing one thousand every quarter.

Finally, when determining how often and where continuous auditing will be performed, the CAE should consider not only the regulatory requirements, but also the degree to which management is addressing the risk exposures and potential impacts. When management has implemented continuous monitoring systems for controls, internal and external auditors can take this into account and decide the extent to which they can rely on the continuous monitoring

GTAG — Implementing Continuous Auditing — 6

processes to reduce detailed controls testing. To rely on the processes, auditors need to consider and assess the following:

- Identification of the specific internal controls addressed.
- Security over access to the monitoring system.
- Response to control anomalies identified.
- Control total reconciliations.
- Audit logs of processing activities.
- Audit logs of changes made to test parameters and thresholds.

Once the tests have been run, the CAE can review the results to identify where problems exist. Control weaknesses are evidenced by transactions that fail the control tests. Increased levels of risk can be identified by comparative analysis (i.e. comparing one process to other processes, one entity to other entities, or running the same tests and comparing results over time.)

One of the practical challenges of implementing a continuous auditing or monitoring system is the efficient response to control exceptions and risks that are identified. When a continuous auditing or monitoring system is first implemented, it is not unusual for a large number of exceptions to be identified, which upon investigation, prove not to be a concern. The continuous auditing system needs to allow the test parameters to be adjusted so that, where appropriate, such exceptions do not result in alerts or notifications. Once the process of identifying such “false positives” is performed, the system increasingly can be relied upon for only identifying control deficiencies or risks of significant concern.

In addition, the nature of the audit response to the identified transactions will vary, and not all will require an audit or immediate action. The results should be prioritized and acted upon accordingly. Details to be maintained should include:

- The results obtained.
- Decisions regarding what action will be taken.
- Who was notified and when.
- The expected response date.

If a transaction was referred to management, the auditor should also request a management response outlining the action plan and date. Once the appropriate action has been taken, the auditor should run the continuous auditing test again to see if the remediation has addressed the control weakness or reduced the level of risk. Subsequent tests should not identify the same problem.

It is vital that everyone understand the rationale for continuous auditing. It is equally important to try to obtain indicators that cannot be manipulated. The CAE must understand and take steps to avoid manipulation, misinterpretation, and “paralysis by analysis.” A key to success is ensuring that the indicators are responsive to changes in risk and controls, easily understood by everyone involved, protected from direct or indirect manipulation without a change to the underlying behavior, and focused on short- and long-term organizational goals.

There are various aspects of security and control to consider in relation to a continuous auditing system. The usual issue of confidentiality of certain information applies, and access to viewing the results of the auditing or monitoring process needs to be restricted and controlled appropriately. Another key area of security and control involves the setting of thresholds and varying test parameters. If the results of the continuous auditing system are to be reliable, there needs to be effective controls, including audit trails, over the changes made. As with any application of CAATs, it is also important to ensure that control totals from the source data systems can be agreed to the totals of transactions tested. Finally, because the continuous auditing tests may identify fraud as well as control weaknesses and risk exposures, the CAE must ensure that the test parameters and results are secure from unauthorized access.

The use of a properly designed continuous auditing application will assist the audit activity in its role of providing assurance that management is maintaining an effective control framework and actively managing risk. However, continuous auditing must remain flexible and responsive to changes in the exposures and the control environment. It is not something that can be implemented and left alone for months. The CAE should review the efficiency and effectiveness of the continuous auditing program periodically. Additional control points or risk exposures may need to be added, and others may be dropped. Thresholds and control tests and parameters for various analytics may need to be tightened or relaxed. During this review, the CAE should also ensure that the results from continuous auditing are included in other management activities, such as ERM, balanced scorecard, and performance measurement and monitoring.

Challenges and Other Considerations

Pre-conditions

Although technology has made data easier to access than before, and computing power makes real-time analysis increasingly feasible, technical hurdles remain:

- Information to be audited must be generated by reliable systems.
- The continuous auditing process must be highly automated with an effective link between the auditor’s system and that of the audited entity.
- Accurate and understandable continuous auditing reports must be developed and be available on a timely basis.
- Auditors must have the proficiency to undertake such audit engagements.

To overcome these challenges, auditors must have the ability to:

- Gain access to relevant data in a timely manner and be capable of normalizing data from disparate systems across the organization.

GTAG — Implementing Continuous Auditing — 6

- Analyze large volumes of data without compromising the system's operational performance.
- Understand the business process sufficiently well to define the appropriate analytics and identify potential risks and key control points.
- Identify the most effective source of the data and control points at which to perform the continuous auditing tests and analyses.
- Perform a comprehensive set of tests and analyses to address key control points and areas of risk and report the results in a timely manner.
- Understand the nature of the test or analysis when investigating exceptions or processes and systems identified as being at risk (i.e. Why are you looking at this?)
- Accumulate and quantifying total risk exposures.
- Monitor and modify the variables used for continuous auditing, tuning the system to produce manageable results.
- Balance the cost and effort against the exposure.
- Prioritize actions.
- Manage the alert notifications.
- Secure access to the continuous auditing system to prevent unauthorized changes to the analysis jobs or threshold/cut-off values.

Access to Personal Information

Although the privacy legislation in many countries permits internal auditors to access personal information for audit purposes, accessing employees' personal information can be a significant issue and must be resolved early in the continuous auditing process. To meet the demands of legislation, the auditor may be required to explain who will have access to the information and how it will be used, stored, and kept secure.

GTAG – Conclusion – 7

In light of today's challenges, it is imperative that CAEs find new ways to enable the internal audit function to respond effectively to the demands of a rapidly changing business environment and the burden of growing regulatory compliance requirements. The integrated approach of continuous auditing and continuous monitoring, enabled by technology, is the key to a sustainable, cost-effective, and resource-efficient solution.

These challenges can be viewed as an opportunity for the internal audit profession and its leaders to provide tremendous value to the organization. Internal auditing is uniquely positioned to not only provide the organization with assurance that it is in compliance with laws and regulations, but also to assist the organization in improving the effectiveness and efficiency of business processes. The return of implementation of continuous auditing will be realized through improvements to an organization's bottom-line results, based on the timely identification of errors, fraud, and the creation of a stronger internal control environment across the enterprise.

GTAG — Appendix A — Example of Continuous Auditing Applied to Accounts Payable — 8

Although continuous auditing can be used in any area of the organization, a simple example involving accounts payable (AP) illustrates the strengths of this approach when applied to a specific audit. The example assumes that there are numerous, separate AP processing centers of different sizes performing similar functions. The example will be used to discuss four main objectives:

- Identification and assessment of risk related to the AP processes.
- Identification of trends related to performance and efficiency.
- Identification of control deficiencies, specific anomalies, and potential frauds.
- Tracking of the implementation of audit recommendations and their effect on accounts payable operations.

In each case, the analysis would consider trends over time and compare the AP section under review to other AP groups within the organization. Benchmarking against external AP operations would add another dimension to the examination.

Risk Identification and Assessment

A wide variety of data-driven and nondata-driven risk factors should be included in the initial risk assessment. A comprehensive evaluation of business performance looks at cost, quality, and time-based performance measures.

- Cost-based measures cover the financial side of performance, such as the labor cost for AP.
- Quality-based measures assess how well an organization's products or services meet customer needs, such as the average number of errors per invoice.
- Time-based measures focus on efficiency of the process, such as the average number of days to pay an invoice.

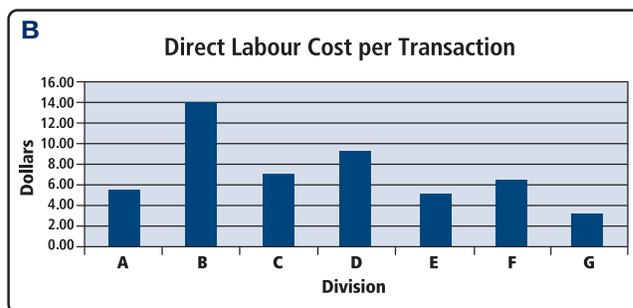
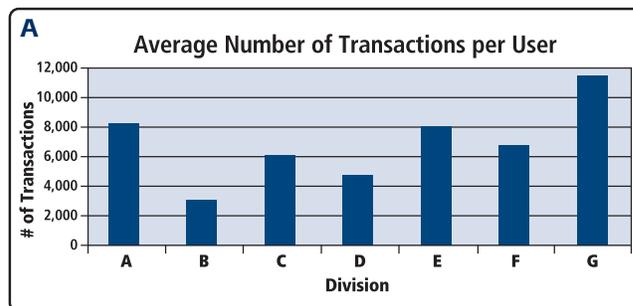
It is also possible to determine, for each AP section, the types of transactions and dollar amounts. For example, look at the number of corrected journal entries and manually produced checks. These are indicators of additional workload. The analysis also will tell you how many different types of transactions are being processed. Generally speaking, there is greater complexity in operations when more transaction types are processed. You also can examine components of the organizational structure such as reporting relationships, number and classification/level of staff, length of time in job, retention rates, and training received. This data should be available from human resources. The combination of this type of information with the transaction types and volumes can help to identify areas of risk, such as understaffing or lack of trained staff to handle complex transaction types.

Trends in Performance and Efficiency

When considering AP, trending data will easily identify performance and efficiency concerns. For example, for each AP operation, continuous auditing can determine:

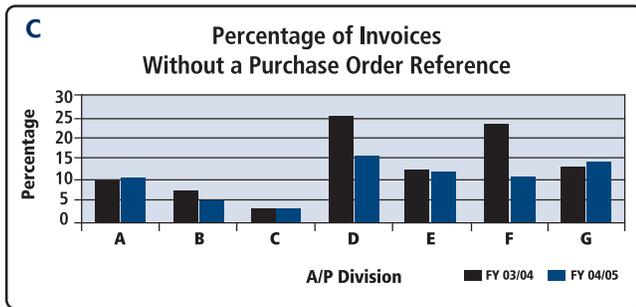
- Number and classification/level of AP staff.
- Number of invoices processed by each user at either end of the spectrum. (Too many or too few can increase risk.)
- Average dollar cost to process an invoice.
- Average number of days to process a payment.
- Percentage of invoices paid late and paid early. (This can be particularly telling if early payment discounts are not taken.)
- Percentage of adjusted entries.
- Percentage of recurring payments or electronic funds transfer payments.
- Percentage of manual checks.
- Percentage of invoices that do not reference a purchase order.
- Percentage of invoices that are less than US \$500. (A purchase card could be used for more efficiency and less cost.)

Efficiency measures allow auditors to compare one audit area to another with a graphic depiction of the results. For example, graphs A and B below illustrate that Division B processes the fewest average transactions per user and incurs the highest direct labor cost per transaction — a clear candidate for operational efficiency improvements.



Analyzing trends can help to identify not only problems, but also areas where improvements have been made. Graph C shows that Division D still has the highest percentage of invoices without a purchase order reference, but the division has made considerable improvements over the previous year, whereas Division G's percentage has gone up.

GTAG – Appendix A – Example of Continuous Auditing Applied to Accounts Payable – 8



Identification of Control Deficiencies, Anomalies, or Potential Fraud

Within AP, possible anomalies and measures of potential fraud include:

- Identification of duplicate payments. (This should include a comparison to previous years to see if operations are improving.)
- Invoices processed against purchase orders that were created after the invoice date (e.g. back-dated purchase orders).
- Number of invoices going to suspense accounts.
- Identification of duplicates in the vendor table or of vendors with names such as C.A.S.H., Mr., Mrs., or vendor with no contact information, phone numbers, or other key information.
- Identification of all functions performed by each user to identify incompatibility or lack of segregation of duties, such as identification of:
 - Vendors that were created by, and only used by, a single AP clerk.
 - Instances where the entry user is the same as the user who approves payment.
 - Instances where the payee is the entry or approving user.

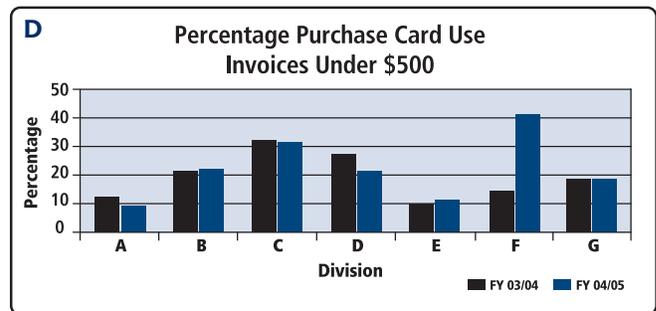
Tracking of Audit Recommendations

The final objective of continuous risk assessment is the tracking of recommendations. The aim is to determine whether management has implemented the recommendations and whether the recommendations are having the desired effect. Possible measures include:

- Evidence of increased use of purchase cards for low dollar transactions (e.g. reduction in percentage of invoices less than \$500 and increase in percentage of purchase card payments less than \$500).
- Reduction of duplicates in the supplier master table.
- Decrease in the number and dollar value of duplicate invoices.
- Improvements in the days-to-pay figures (e.g. reduction in late payment charges; more opportunities for early payment discounts).

- Improved operations (e.g. lower cost per invoice, more use of electronic funds transfer (EFT) payments).
- Tightened role-based user access limiting the opportunities for fraud, waste, and abuse (e.g. fewer instances of a lack of segregation of duties).

Graph D shows how continuous risk assessment can be used to determine whether AP operations in each division have successfully implemented the recommendation calling



for purchase cards to be used for low dollar transactions.

With millions of transactions entered annually in a large number of AP processing centers, the audit activity can be effective and efficient with the use of continuous auditing technology. Continuous auditing helps define the audit objectives, select offices for on-site audit work, and identify control weaknesses and anomalies. Finally, continuous auditing allows the auditors to follow-up on the implementation of the audit recommendations electronically, without having to travel to various offices to perform a manual review of transactions.

American Institute of Certified Public Accountants (AICPA) – SAS

- SAS #47, Audit Risk and Materiality in Conducting Audits.
- SAS #54, Illegal Acts by Clients.
- SAS #56, Analytical Procedures.
- SAS #78, Amendment to SAS #55, Consideration of Internal Control in a Financial Statement Audit.
- SAS #80, Amendment to SAS #31, Evidential Matter.
- SAS #94, The Effect of Information Technology on the Auditor's Consideration of Internal Controls in a Financial Statement Audit.
- SAS #99, Considerations of Fraud in a Financial Statement Audit.

The Institute of Internal Auditors

- Standard 1210: Proficiency.
- Practice Advisory 1210.A2-1: Identification of Fraud.
- Practice Advisory 1210.A2-2: Responsibility for Fraud Detection.
- Practice Advisory 2310-1: Identifying Information.
- *GTAG Information Technology Controls.*
- *GTAG Change and Patch Management Controls: Critical for Organizational Success.*

International Federation of Accountants – International Standard of Auditing (ISA)

- ISA #240, The Auditor's Responsibility to Consider Fraud in the Audit of Financial Statements.

The use of concepts, methodology, and technology required for continuous auditing has not been applied consistently across internal audit departments. Some auditors are leaders in adopting and deriving the maximum benefit from continuous auditing, while others have not even started on the process of implementing it. Most organizations exist somewhere in the middle of these two extremes.

Typically, the use of continuous auditing falls into one of three main categories: introductory, moderate, integrated/advanced. Each category can be characterized according to the degree to which continuous auditing has been implemented and integrated with audit processes.

The CAE should be aware of where the audit department currently is in terms of continuous auditing and where it would like to be. Part of the process of moving toward a more advanced use of continuous auditing includes an assessment of internal auditors' skills and knowledge. Varying levels of IT knowledge are needed throughout the organization for evaluating and improving the effectiveness of risk management, control, and governance processes. Knowledge of business systems, the related risks and control issues, and the ability to use IT as a resource in the performance of continuous auditing is essential.

The CAE can use the following level descriptions to self-assess the degree to which the audit department has adopted and implemented continuous auditing.

Introductory Level

Audit departments at the introductory level have not really started to employ continuous auditing methodologies and technologies. Although some auditors may have accrued some benefits from the use of computer technology, most risk and control assessment tasks are still performed manually. At the introductory level, data analysis may be used to support individual auditing but this is on an ad hoc basis. The analyses are run once, and the results are used only to address specific audit objectives.

Introductory use can be characterized by:

- A general understanding of business risks and controls.
- Ad hoc use of IT to search for anomalies or exceptions.
- Point-in-time assessments of transactions to address specific audit objectives.
- Risk assessments that rely on qualitative criteria and lack quantification.
- Control assessments that are performed manually.
- Technology use that's not integrated with the audit planning process, audit risk assessment, or evaluation of controls.

At the introductory level, the CAE does not have a plan to see the audit department moving forward in its efforts to implement continuous auditing. Technology is not planned for, or considered in either the short- or long-range plans of the audit department. Typically, the use of technology is piecemeal and intended to deal with one problem.

Moderate Level

At the moderate level, continuous auditing techniques are having an impact on the actual audits being conducted. However, the impact is still somewhat limited, and its use is not applied or managed consistently. Often, it may be only a few auditors who are making use of continuous auditing techniques, and their efforts may not be sponsored by the CAE. In addition, senior management of the company may not be aware of the type or extent of continuous auditing used by these auditors.

The types of audits performed, the results achieved, and the methodology employed have not changed — only the use of technology to perform certain functions. Technology may be planned for, but there is no vision for where the audit department's use of continuous auditing is going. In addition, the application of continuous auditing is not integrated with the audit planning process or the assessment of risk and control issues.

Moderate use can be characterized by:

- A basic understanding of the threats and vulnerabilities associated with automated business systems and associated controls.
- Audit teams that have the skills and knowledge necessary to extract and use data from key business systems.
- An audit department that has purchased and is using IT tools to perform assessments and tests.
- Audit tests that are run to search transactions for evidence of IT risks and vulnerabilities or control deficiencies on an ad hoc basis.
- Detected symptoms that are related to business systems to identify causes and make recommendations.
- The enterprisewide audit plans may include some quantitative and qualitative criteria, but they are updated only during the annual audit planning process.

These audit departments are at a critical point. The use of continuous auditing may regress if key individuals leave or the use of continuous auditing is not made an integral part of the audit process.

Integrated/Advanced Level

At this level, the CAE and all auditors recognize the importance of technology and continuous auditing. The implementation and maintenance of continuous auditing has sufficient resources — human and financial — and the technology is integrated in the overall audit processes.

Auditing has become a continuous process, and auditors perform risk and control assessments by examining detailed transactions for anomalies or exceptions and by examining trends. The results are used to trigger alarms, which are prioritized and acted upon quickly. At this level, the nature of the audit activity has changed. The inputs, outputs and processes are not the same as that of an audit department that has not implemented continuous auditing. The types of audits performed, planning cycle, cycle time,

and many other aspects are affected by the implementation of continuous auditing.

Integrated/advanced use can be characterized by:

- A knowledge of the key business processes and associated systems and a good understanding of the risks and control issues.
- The identification of critical control points and control rules and exceptions.
- The audit department having identified key risk categories and data driven indicators of risk.
- The performance of risk and control assessments in real time or near real time for key business processes.
- Key business systems that are analyzed for exceptions/anomalies at the transaction level and for trends indicating emerging risks.
- An enterprisewide audit planning process that includes data-driven indicators of risk and performance.
- Audits that all strive to identify data-driven indicators for audit recommendations, which are analyzed to assess management's implementation of the recommendations.
- Continuous auditing results that are integrated in all aspects of the audit process and results that are linked to ERM, balanced scorecard, and continuous improvement initiatives.
- Auditors that evaluate and consider management's monitoring processes when performing continuous auditing.
- Continuous auditing that is planned for, managed, and evaluated for continuous improvement.

Today, not many audit departments are at the integrated/advanced level of continuous auditing. But the path to get there can be adopted incrementally starting with the identification of key business systems and controls. Initial applications on continuous auditing can be run on a periodic, rather than a continual, basis. It's most important for CAEs to understand where the audit department is currently, to develop a vision for where they'd like it to be, and to plan for how to get there.

David Coderre is manager, Continual Auditing for the audit and evaluation branch of the Royal Canadian Mounted Police. He has more than 20 years of experience in the informatics field in the university environment and private and federal government sectors. He is responsible for the effective and efficient use of informatics hardware and software as an audit tool; he performs analyses to support the scope and objectives of individual auditing; and he supports the development of the annual audit plan by identifying and assessing risks. Coderre has responded to the requirements of hundreds of audits by working with audit teams to develop data-driven methods of addressing audit scope and objectives. Previous results include: an inventory audit that found more than US \$100 million in obsolete inventory; the audit of an AP function that identified close to US \$5 million in inefficiencies and more than US \$1 million in duplicate payments; and a contracted maintenance audit that uncovered millions of dollars of fraudulent transactions.

Coderre also authored the books *CAATTs and Other BEASTs for Auditors* (Version 3, 2005) and *Fraud Detection: A Revealing Look at Fraud* (Version 2, 2004), which describes techniques for using data analysis software to detect fraud, waste, and abuse. In 2001, he published *The Fraud Toolkit*, a combination of software and written text that contains a series of cases and scripts specifically designed to address fraud. He has also written many articles for international audit magazines, including *Internal Auditor*, *The EDP Audit*, and *Control and Security Newsletter* (EDPACS), the UK Journal of Auditing.

Contact Information:
Royal Canadian Mounted Police
Audit and Evaluation Branch
295 Coventry Rd. – 2nd Floor
Ottawa, Ontario
K1A0R2, CANADA
+1-613-993-1189
Dave_Coderre@hotmail.com

About the Project Team

Primary Author:

David Coderre, Manager, Continual Auditing,
Royal Canadian Mounted Police

Project Manager:

Peter Millar, Director, Product Marketing,
ACL Services Ltd.

Project Sponsor:

John Verver, Vice President, Professional Services,
ACL Services Ltd.

Subject Matter Experts:

John G. Verver, Vice President, Professional Services,
ACL Services Ltd, Vancouver, Canada

J. Donald Warren Jr. , Professor of Accounting and
Director, Center for Continuous Auditing, Department
of Accounting & Information Systems, Rutgers
University, Newark, N.J., USA

Contributors:

Brian Aiken, Director General Audit and Evaluation,
Royal Canadian Mounted Police, Ottawa, Canada

Richard B. Lanza, President, Cash Recovery Partners
LLC, Lake Hopatcong, N.J., USA

Sylvain Michaud, Director Internal Audit,
Royal Canadian Mounted Police, Ottawa, Canada

Robert, L. Onions, Director, Eclectics Ltd,
Bude, England

Mary Persson, Director Methodology, Royal Canadian
Mounted Police, Ottawa, Canada

René-Pierre Tremblay, Director Management
Review/Quality Assurance, Royal Canadian Mounted
Police, Ottawa, Canada

GTAG – References – 12

- Assurance Services Within the Auditing Profession*, Glen L. Gray and Maryann, J. Gray, The IIA Research Foundation, Altamonte Springs, Fla., USA, 2000.
- “Beyond Traditional Audit Techniques,” Paul E. Lindow and Jill D. Race, AICPA, *Online Journal of Accountancy*, July 2002 / Volume 194, No. 1.
- Building and Implementing a Continuous Controls Monitoring and Auditing Framework – A White Paper*, John G. Verver, ACL Services, 2005.
- CAATTs and Other BEASTs for Auditors*, David G. Coderre, Global Audit Publications, Vancouver, Canada, 1998.
- CoBIT, IT Governance Institute and the Information Systems Audit and Control Association.
- Continuous Auditing*, Canadian Institute of Chartered Accountants, Toronto, Canada, 1999.
- “Continuous Auditing: The Audit of the Future,” Zabihollah Rezaee, Rick Elan, and Ahmad Sharbatoghlie, *Managerial Accounting Journal* 16/3, pp 150-158, MCB University Press.
- Continuous Auditing: Implications of the Current Technological, Regulatory and Corporate Environment*, J. Donald Warren Jr., Texas A&M University, May 2004.
- Continuous Auditing: Potential for Internal Auditors*, J. Donald Warren Jr. and Xenia L. Parker, The IIA Research Foundation, Altamonte Springs, Fla., USA, 2003.
- Continuous Monitoring: An Effective Strategy for Effective Controls*, John G. Verver, The 16th Annual Super Strategies: Audit Best-Practices Conference, MIS Training Institute, 2005.
- “Detecting Accounts Payable Abuse Through Continuous Auditing,” Larry Potla, *ITAudit*, The IIA, Altamonte Springs, Fla, USA, Volume 6, Nov. 2003.
- Enterprise Risk Management: An Analytical Approach*, Tillinghast-Towers Perrin, 2000.
- Enterprise Risk Management – Integrated Framework*, COSO, 2004.
- Financial Post*, Andrew Parker, Tuesday, May 17, 2005.
- Fraud Detection: A Revealing Look at Fraud*, David G. Coderre, Ekaros, Vancouver, Canada, 2004.
- The Future of Continuous Assurance and Risk Management*, Tim J. Leech, Paisley Consulting, 2005.
- GTAG Information Technology Controls*, The IIA, Altamonte Springs, Fla, USA, March 2005
- Internal Auditing in Europe*, ECIIA, February 2005.
- Internal Control – Integrated Framework*, COSO, 1992.
- Professional Practices Framework*, “Guidance on Implementing Auditing Standard #2,” The IIA Research Foundation, Altamonte Springs, Fla., USA, 2004.
- Report from The IIA’s 2005 International Conference CAE Roundtable Discussion, July 2005.
- Sarbanes-Oxley Implementation Costs*, A.R.C. Morgan, February 2005.
- Sawyer’s Internal Auditing (5th Edition): The Practice of Modern Auditing*, Lawrence B. Sawyer, Mortimer A. Dittenhofer, and James H. Scheiner, Altamonte Springs, Fla., USA, 2003.
- SOX Compliance and Automation: A Benchmark Report*, Aberdeen Group, March 2005.
- SOX Decisions for 2005: Step Up Technology Investments*, John Hagerty, AMR Research, January 2005
- Survey on SOX 404 Implementation, Financial Executives International, March 2005.
- Technology Risk and Controls: What You Need to Know*, Protiviti Independent Risk Consulting, 2004.

GTAG – Preview of GTAG 4

Privacy - Operational and Auditing Issues

The next publication for chief audit executives (CAEs) in the Global Technology Audit Guide (GTAG) series deals with privacy risks and auditing.

This GTAG will deal with the spectrum of privacy challenges today's organizations face and how auditors need to respond. Information needs to be secured, but even more so when it relates to individuals; increased care has to be taken to avoid litigation or damaging reputation. Balancing customer expectations, business needs, and manifold legal requirements becomes increasingly complex when dealing with sensitive data or a global customer base.

The objective of the guide is to outline privacy concepts and issues that will help CAEs, their peers, and their staff deal with privacy issues throughout planning, preparing and performing audits. Because audit's role requires assessing risks and providing assurance to the organization, auditors cannot ignore the potential impact of privacy failures and misconceptions on the organization. This guide allows readers to understand the issues at stake, to efficiently locate key risks, and to provide assurance and advice for efficient compliance to privacy needs.

What is the Internal Auditor's Role?

Implementing adequate privacy is primarily a business issue; IT plays a facilitating role and internal auditing itself can give assurance and advice.

The guide will provide a generic outline of privacy principles based on the auditing profession's most current material and the agenda-setting, rule-making bodies. It will review privacy safeguards, frameworks, and cover a wide range of business issues and how to determine and evaluate privacy risks. Key sector and industry issues (financial services, communications, media, health care, government, etc.) will be outlined. Also in this publication, technical and organizational aspects, privacy controls, and best practices including, a reference to COSO's ERM.

Privacy has several implications to auditing. According to The IIA's *International Standards for Professional Practice of Internal Auditing (Standards)* and Practice Advisories, privacy has to be reflected in the audit planning, individual assignment pre-assessments and the handling of assignment files and reports. This GTAG will elaborate on how to deal with privacy within the audit process and also provide a generic outline for a privacy audit program.

The GTAG's appendix will feature the "Top Ten Questions to Ask on Privacy," an example audit program and a global, up-to-date reference.

Watch out for this new GTAG offering in late 2005.

IIA / DELOITTE & TOUCHE 2006 TRAINING SCHEDULE

Auditing JD Edwards

San Francisco, CA March 6–10
Chicago, IL June 5–9
Santa Ana, CA September 18–22
Chicago, IL December 4–8

Auditing Oracle Applications

Santa Ana, CA February 13–17
Chicago, IL April 3–7
San Francisco, CA June 5–9
Chicago, IL August 21–25
Santa Ana, CA October 23–27

Auditing PeopleSoft

Chicago, IL February 20–24
Santa Ana, CA May 8–12
Chicago, IL August 7–11
San Francisco, CA November 6–10

Computer-assisted Audit Techniques

San Francisco, CA April 24–26
Chicago, IL October 16–18

Enterprise Software Implementation for Auditors

San Diego, CA March 1–3
Boston, MA July 26–28
Washington, DC October 11–13

Information Security Concepts

Orlando, FL March 27–31
Orlando, FL May 22–26
Atlanta, GA October 30–November 3

Internet Security for IT Auditors

Baltimore, MD April 12–14
Las Vegas, NV August 7–9
San Antonio, TX October 18–20

Introduction to Auditing SAP R/3

Chicago, IL February 6–10
San Francisco, CA April 3–7
Santa Ana, CA June 19–23
Chicago, IL September 11–15
Santa Ana, CA November 6–10

Introduction to IT Auditing

Phoenix, AZ January 23–27
Orlando, FL March 27–31
Chicago, IL May 8–12
Boston, MA July 24–28
San Diego, CA August 14–18
Orlando, FL September 25–29
Phoenix, AZ November 6–10
Las Vegas, NV December 11–15

IT Audit Symposium: An Overview for CAEs and Audit Management

Atlanta, GA February 10
New York, NY June 16
Denver, CO September 15
Phoenix, AZ November 10

IT Auditing: A Comprehensive View for CAEs and Audit Management

Las Vegas, NV March 6–9
Orlando, FL May 22–25
Denver, CO September 11–14
San Antonio, TX October 16–19

IT Auditing: Beyond the Basics

Las Vegas, NV March 6–10
Vancouver, BC July 10–14
Palm Beach, FL August 28–September 1
Orlando, FL December 4–8

SAP R/3 Technical Audit

Santa Ana, CA March 6–10
Chicago, IL May 15–19
San Francisco, CA August 7–11
Santa Ana, CA October 16–20
Chicago, IL December 11–15

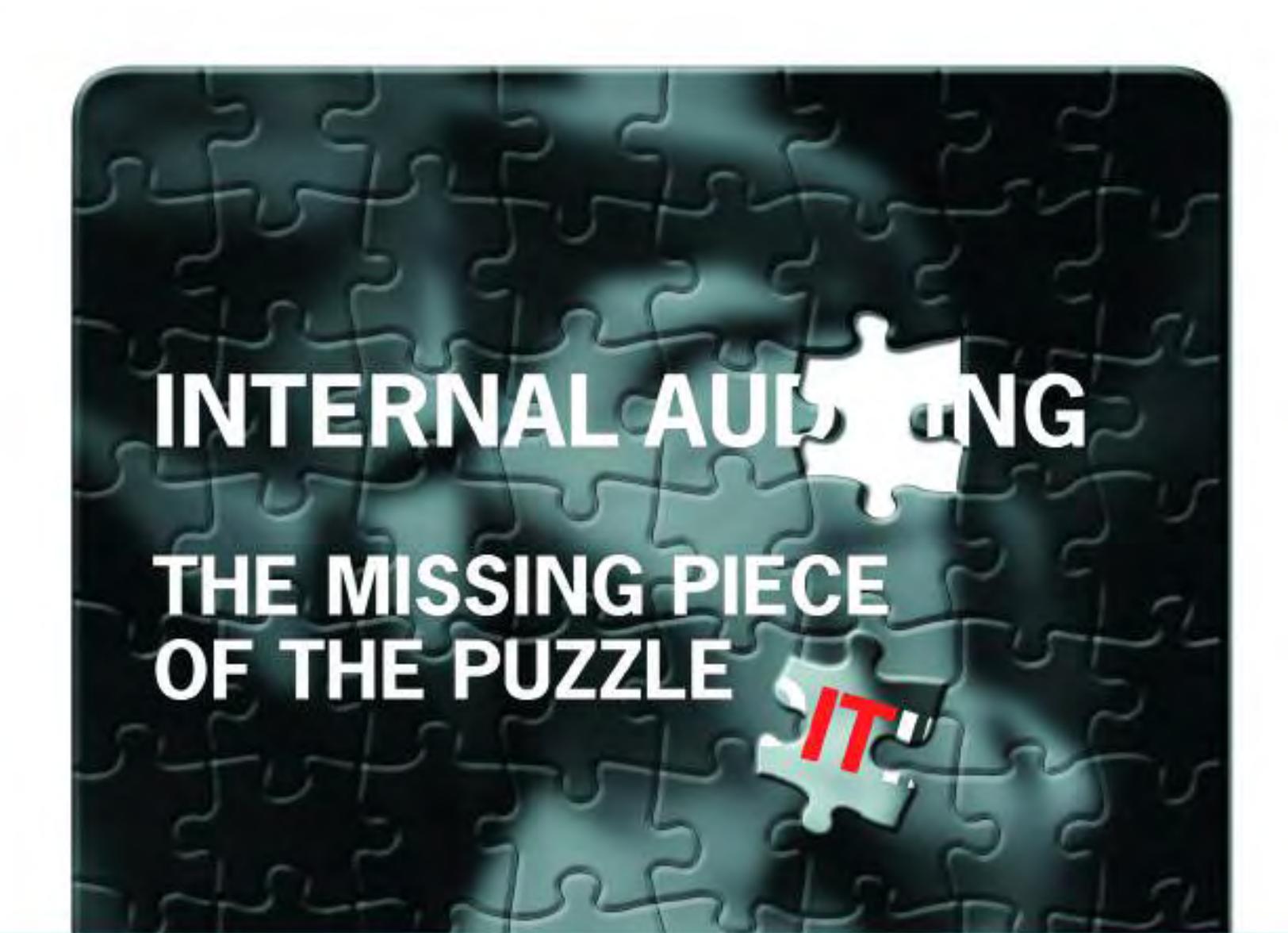
For more information visit
www.theiia.org/Seminars or +1-407-937-1111

Deloitte.



IIA TRAINING
Never Stop Learning

> We know it > We do it > We teach it



INTERNAL AUDITING

THE MISSING PIECE OF THE PUZZLE

THE IIA'S INFORMATION TECHNOLOGY CONFERENCE

February 13–15, 2006

Disney's Contemporary Resort

Lake Buena Vista (Orlando), Florida, USA

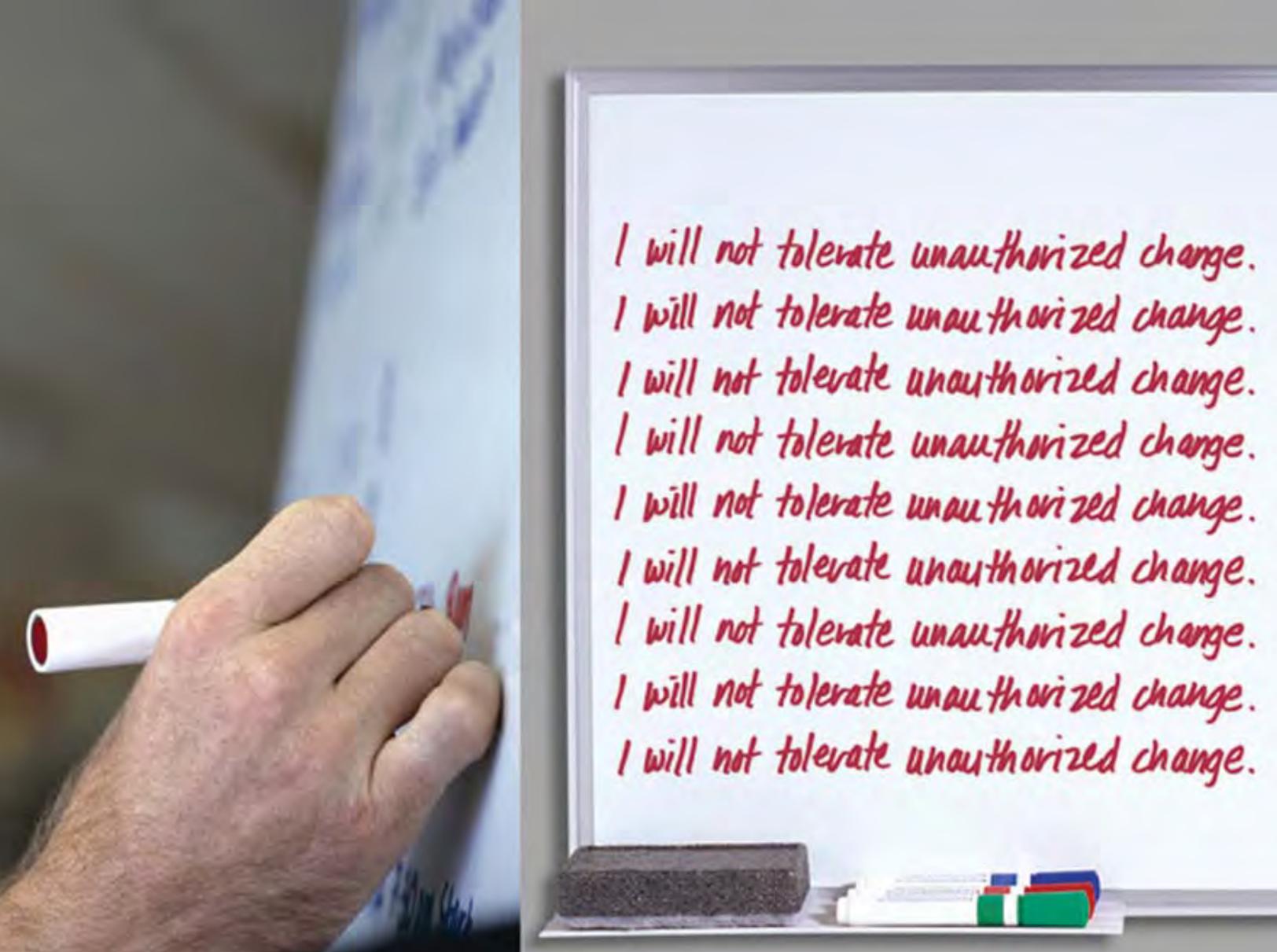
TECH2006

This conference is a must for internal audit professionals at all levels.



IIA TRAINING
Never Stop Learning

+1-407-937-1111 / www.theiaa.org/Training



IF ONLY THE PENALTY FOR NONCOMPLIANCE WAS THIS SIMPLE.

TRIPWIRE

Audit Change. Prove Control.

"Tripwire is one of our most valuable tools to assure once and future compliance."

—Barak Engle, CSO, InStorecard

Unauthorized change is something you can't entirely eliminate. But with the right independent detective controls, you can detect every change across all your servers, desktops, network devices, directory servers, and other infrastructure components.

That independent detective control is Tripwire change auditing. We're the antidote for out-of-control change. We give you a single point of control for detecting, reconciling and reporting change activity across the enterprise.

Find out why more than 4500 customers rely on us to achieve compliance in a wide range of regulatory environments. Sign up for our latest webcast at www.tripwire.com/audit.



*Continuous Auditing:
Implications for Assurance,
Monitoring, and Risk Assessment.*

This guide focuses on assisting chief audit executives in identifying what must be done to make effective use of technology in support of continuous auditing. It provides audit guidance on how to use continuous auditing to benefit the organization by significantly reducing instances of error and fraud, increasing operational efficiency, and improving bottom-line results through a combination of cost savings and a reduction in overpayments and revenue leakage.

What is GTAG?

Prepared by The Institute of Internal Auditors, each Global Technology Audit Guide (GTAG) is written in straightforward business language to address a timely issue related to information technology management, control, or security. GTAG is a ready resource series for chief audit executives to use in the education of members of the board and audit committee, management, process owners, and others regarding technology-associated risks and recommended practices.



**The Institute of
Internal Auditors**

Order Number: 1010
IIA Member US \$25
Nonmember US \$30
IIA Event US \$22.50

ISBN 0-89413-586-4

