GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance

2nd Edition

The Institute of Internal Auditors

Global Technology Audit Guide (GTAG®) 3
Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance

2nd Edition

March 2015

GTAG — Table of Contents

Executive Summary

An evolving regulatory environment, growing globalization, market pressure to improve operations, and rapidly changing business conditions are creating a need for organizations to develop continuous auditing programs aimed at both financial and operational data. Such programs support internal audit's ability to provide continuous assurance of effective risk management and control to those charged with governance.

Continuous auditing comprises ongoing risk and control assessments, enabled by technology and facilitated by a new audit paradigm that is shifting from periodic evaluations of risks and controls based on a sample of transactions, to ongoing evaluations based on a larger proportion of transactions. Continuous auditing also includes the analysis of other data sources that can reveal outliers in business systems, such as security levels, logging, incidents, unstructured data, and changes to IT configurations, application controls, and segregation of duty controls.

Through continuous auditing, internal audit departments can realize significant increases in efficiency and heightened levels of insight. Key steps to implementing continuous auditing include:

1. Establishing a continuous auditing strategy.
2. Acquiring data for routine use.
3. Constructing continuous auditing indicators (ongoing risk assessment and ongoing control assessment).
4. Reporting and managing results.

However, to unlock the full power of a continuous auditing program, it must be coordinated with the continuous monitoring programs conducted by the organization's operational and oversight management functions.

Organizations ideally use a three lines of defense risk management and control framework.[1] The first line of defense comprises operational management functions that own and manage risks. The second line of defense includes management functions such as compliance and risk management departments that oversee risks. The third line of defense is the internal audit function, which provides objective assurance over the effectiveness of governance, risk management, and internal control. Continuous monitoring encompasses ongoing efforts by the first and second lines of defense to ensure that policies, procedures, and business processes are operating effectively. It involves identifying applicable control objectives and assurance assertions, and establishing automated tests to highlight activities and transactions that fail to conform to expected norms. Internal audit can provide the organization with continuous assurance by performing ongoing testing of continuous monitoring concurrently with its continuous auditing activities.

Continuous auditing can be applied to audit plan development, audit engagement support, and follow-up on audit findings. Chief audit executives (CAEs) should be aware that continuous auditing will change the nature of evidence, timing, procedures, and level of effort required by internal auditors. Coordinating continuous auditing, continuous monitoring, and audit testing of continuous monitoring helps internal audit and management maximize their respective returns on investment and achieve compliance objectives, and it provides the opportunity to enhance the organization's overall health and competitiveness.

A coordinated effort results in the timely notification of gaps and weaknesses in risk management and control, and creates an environment whereby timely follow-up and treatment are improved. Coordinating the organization's continuous monitoring and continuous auditing efforts can improve overall organizational understanding of data, risk, and control and maximize internal audit's ability to provide senior management and the board with effective continuous assurance.

[1] The IIA Position Paper, The Three Lines of Defense in Effective Risk Management and Control.

Introduction

Internal audit's approach to evaluating the effectiveness of risk management and internal control traditionally has been retrospective, with testing of controls performed on a cyclical basis — often months after business activities have occurred. Two factors are driving internal audit's efforts to modify its historically retrospective approach:

- The organization needs to keep pace with the business by responding more timely to accelerated rates of change and emerging risks.
- Advancements in technology have enabled ongoing risk assessments and ongoing control assessments.

The first edition of this guidance, *The IIA's Global Technology Audit Guide (GTAG®) 3: Continuous Auditing – Implications for Assurance, Monitoring, and Risk Assessment*, focused on transactional monitoring and established the alignment between continuous auditing and The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Internal Control–Integrated Framework* (1992). This second edition relates continuous auditing to the three lines of defense in effective risk management and control and expands its focus to include not only transactional data, but also other data sources, such as security levels, logging, incidents, unstructured data, and changes to IT configurations, application controls, and segregation of duty controls.

Business Significance

In many organizations, management and the board are showing signs of fatigue from actual or perceived duplication or overlap of reviews of risk management and controls among the three lines of defense. Continuous auditing has the potential to mitigate this fatigue by:

- Optimizing the balance between the review efforts of internal audit and management.
- Promoting a more efficient use of organizational resources.
- Reducing the cost of assessing and providing assurance over the adequacy of internal controls.
- Providing an ongoing evaluation of risks and controls.
- Providing timely reporting of gaps and weaknesses, enhancing the opportunity for prompt corrective action.
- Providing flexibility necessary to prioritize remediation.
- Promoting better understanding of business performance, risks, and compliance.
- Enabling internal audit to provide continuous assurance regarding controls, risks, and opportunities.

Related IIA Guidance

International Professional Practices Framework (IPPF) guidance related to continuous auditing, continuous monitoring, and continuous assurance includes:

Standard 1210: Proficiency

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

Standard 2010: Planning

The CAE must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.

Standard 2120: Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Standard 2130: Control

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

> 2130. A1 – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:
> - Achievement of the organization's strategic objectives.
> - Reliability and integrity of financial and operational information.
> - Effectiveness and efficiency of operations and programs.
> - Safeguarding of assets.
> - Compliance with laws, regulations, policies, procedures, and contracts.

Standard 2320: Analysis and Evaluation

Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.

Practice Advisory (PA) 2320-4: Continuous Assurance

GTAG 14: Auditing User-developed Applications

GTAG 16: Data Analysis Technologies

Definitions of Key Concepts

First Line of Defense — operating management functions that own and manage risks.

Second Line of Defense — functions that oversee risks, such as compliance and risk management.

Third Line of Defense — an internal audit function that provides independent assurance.

Computer-assisted Audit Techniques (CAATs) — automated audit techniques, such as generalized audit software, utility software, test data, application software tracking and mapping, and audit expert systems, that help internal auditors directly test controls built into computerized information systems and data contained in computer files (*Internal Auditing Assurance & Advisory Services*, 3rd Ed., The IIA Research Foundation).

Configuration — control settings, security levels, parameters, and reference data that enforce authorization, accuracy, and completeness of transaction processing. Configuration choices affect system function, performance, and automated controls.

Continuous Assurance — performed by internal audit, continuous assurance is a combination of continuous auditing and testing of first and second lines of defense continuous monitoring.

Continuous Auditing — the combination of technology-enabled ongoing risk and control assessments. Continuous auditing is designed to enable the internal auditor to report on subject matter within a much shorter timeframe than under the traditional retrospective approach.

Continuous Monitoring — a management process that monitors on an ongoing basis whether internal controls are operating effectively (PA 2320-4: Continuous Assurance).

Ongoing Control Assessment — the ongoing evaluation of internal controls against a baseline condition and subsequent changes to control configurations, through the use of technology-based audit techniques.

Ongoing Risk Assessment — the ongoing identification and assessment of risks to the achievement of business objectives through the use of technology-based audit techniques.

Technology-based Audit Techniques — any automated audit tool, such as generalized audit software, test data generators, computerized audit programs, specialized audit utilities, and CAATs (*The IIA's International Standards for the Professional Practice of Internal Auditing*).

Transactional Data — dynamic detailed data flow normally related to a business process or an economic event such as an order, invoice, or payment.

Unstructured Data — data that is not restricted to a fixed field in a spreadsheet or database. Examples of unstructured data that can be interrogated using continuous auditing and continuous monitoring techniques include text, audio, video, and multimedia data.

Roles and Responsibilities

The performance and coordination of continuous auditing and continuous monitoring to provide continuous assurance require a clear understanding of roles and responsibilities, as outlined in Table 1.

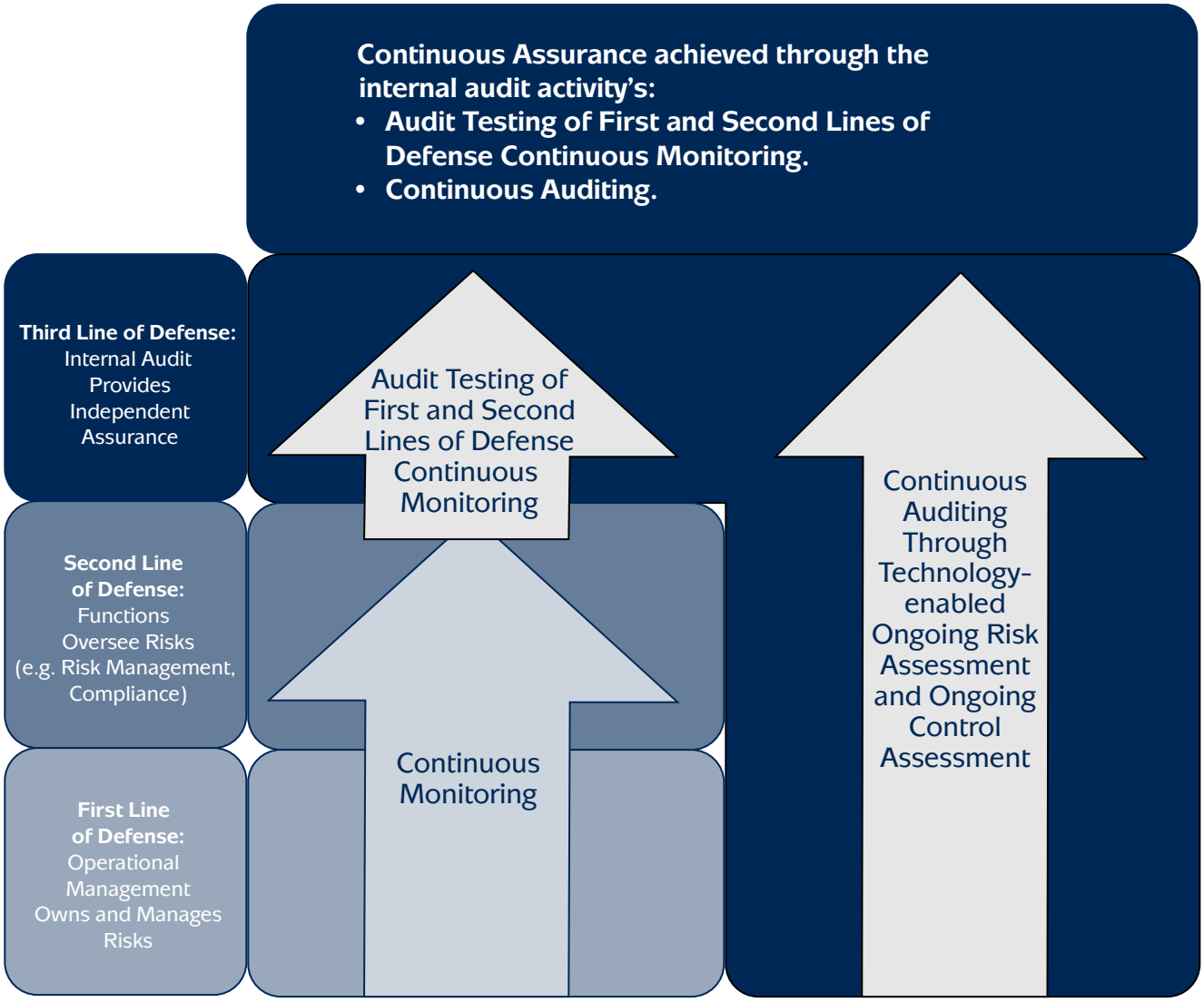
Table 1: Continuous Assurance Roles and Responsibilities

ROLE	RESPONSIBILITIES
CAE	• Establish credibility for continuous auditing activities by ensuring the capability of internal auditors and the sufficiency of their tools, data security arrangements, and budget. • Educate internal auditors, senior management, and the board on the roles and responsibilities of the internal audit activity and management. • Commit to a multi-year strategy to grow support from stakeholders. • Communicate results of internal audit's assessment of the effectiveness of continuous monitoring.
Internal Audit (Third Line of Defense)	• Plan continuous auditing jointly with first and second lines of defense. • Perform continuous auditing: o Relate analytics to assertions and business objectives. o Align risk factors and control activities. o Add value as a trusted adviser by assessing emerging enterprise risks. • Perform audit testing of continuous monitoring. • Provide continuous assurance in connection with audit objectives such as completeness, accuracy, and security. • Maintain effective data security arrangements.
Management (First and Second Lines of Defense)	• Design and perform continuous monitoring to assess the adequacy and effectiveness of risk management and control. • Draw on process expertise and act on risk. Develop and implement management resolutions that address root causes. • Shorten the time to management action.

Foundational Continuous Assurance Framework

The foundational or basic continuous assurance framework encompasses internal audit's continuous auditing process and audit testing of continuous monitoring. As the third line of defense in effective risk management and control, internal audit strives to detect areas of concern within the control framework and, in turn, provide the organization with the highest practicable level of objective assurance.

Figure 1: Foundational Continuous Assurance Framework



Continuous Auditing

Continuous auditing is achieved through ongoing risk and control assessments enabled by technology-based audit techniques such as generalized audit software, spreadsheet software or scripts developed using audit-specific software, specialized audit utilities, CAATs, commercially packaged solutions, and custom-developed production systems. Technology-based audit techniques should be flexible and scalable to play a key role in optimizing:

- Timely identification of exceptions and anomalies.
- Analysis of patterns and trends.
- Detailed transaction analysis against cut-off thresholds.
- Testing of controls.
- Comparative analysis among peers.

Continuous auditing provides a way to identify risk indicators and evaluate risk parameters across IT operations, IT applications, and business processes by analyzing systems for changes, security, incidents, outliers, and transactions. Continuous auditing enhances the ability of internal auditors to comment on the availability and utility of data, understand application controls, and optimize business processes through automation. When deployed effectively, continuous auditing:

- Is focused on audit objectives and assertions such as completeness, accuracy, and authorization to determine the reliability of the information decision makers use.
- Can detect emerging areas of risk and control weakness.

Under the foundational continuous assurance framework (see Figure 1), there is no overlap between continuous auditing and continuous monitoring, and continuous auditing can be performed even if continuous monitoring does not exist in the first and second lines of defense. However, opportunities for continuous monitoring exist wherever there are opportunities for continuous auditing. An opportunity for an audit observation or recommendation may exist if continuous monitoring opportunities are present but are not being performed by management.

Ongoing Risk and Control Assessments

Ongoing risk and control assessments should be designed to work together to sustain assurance and potentially lengthen the time between traditional audit engagements.

Ongoing Risk Assessment

Ongoing risk assessment should include a review of the results of management's monitoring efforts, including leading indicators, performance measures, quality control, and segregation of duties. Ongoing risk assessment continually identifies and assesses risks by using technology-based audit techniques to:

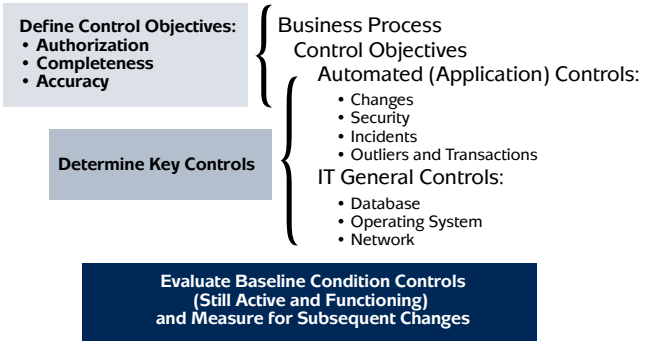
- Examine and analyze trends, comparisons, and outliers within a single process, as compared with its own past performance and against other processes or systems operating within the enterprise.
- Correlate and analyze outliers to show how well management is responding to risks and provide a forward-looking view on emerging risks.
- Highlight potential exposures for focus of audit scoping (periodic and real time).
- Detect outliers in business units, geographies, or processes that may be taking on increased risk or experiencing atypical rates of change.
- Highlight areas where controls are nonexistent or not performing adequately, prompting auditors to perform more thorough control assessments in specific areas.
- Manage business critical spreadsheets and other user-developed applications.[2]
- Predict or anticipate future risks.

Ongoing risk assessment results serve as inputs for the audit plan and ongoing control assessment activities.

Ongoing Control Assessment

An ongoing control assessment continually evaluates internal controls against a baseline condition and subsequent changes to control configurations, and considers the interrelationship of automated controls, IT general controls, and manual controls as illustrated in Figure 2. In each case, the auditor should look for unusual patterns or outliers. Ongoing control assessment enables CAEs to provide management with an early warning of control violations or deficiencies.

Figure 2: Ongoing Control Assessment



[2] For more information, see *GTAG 14: Auditing User-developed Applications*.

Ongoing control assessments need not run in real-time. The frequency of analysis should be determined by the level of risk, the business process cycle, and the degree to which management is monitoring the controls. For example:

- Purchase card analytics might be run once a month, upon receipt of the purchase card transactions from the credit card company.
- Payroll might be run every pay period, in sync with direct deposit transactions.
- Tests for duplicate invoices and payments might be run every day.
- Changes to automated controls tend to be infrequent and might be monitored in sync with the IT routine release cycle.
- Operating system patching might be scanned quarterly.

In some cases, an auditor may perform the initial control testing and transition the ongoing monitoring to management.

Ongoing control assessment results, organized by process, should:

- Support audit objectives.
- Communicate:
  - Conditions of key controls, such as security capabilities.
  - Changes to automated controls.

Continuous Monitoring

Management should own and perform continuous monitoring. Many of the techniques management uses to continuously monitor controls are similar to continuous auditing techniques used by internal auditors. Continuous monitoring principles include:

- **Purpose** – consider the business objective and critical success factors.
- **Risk** – determine likely obstacles that would inhibit the organization's success.
- **Response** – align diverse sources of data to discover and corroborate emerging risks such as configurable conditions, changes, event logging, financial transactions, and unstructured data.
- **Timing** – detect control issues in real time.
- **Action** – track deficiencies for corrective action.

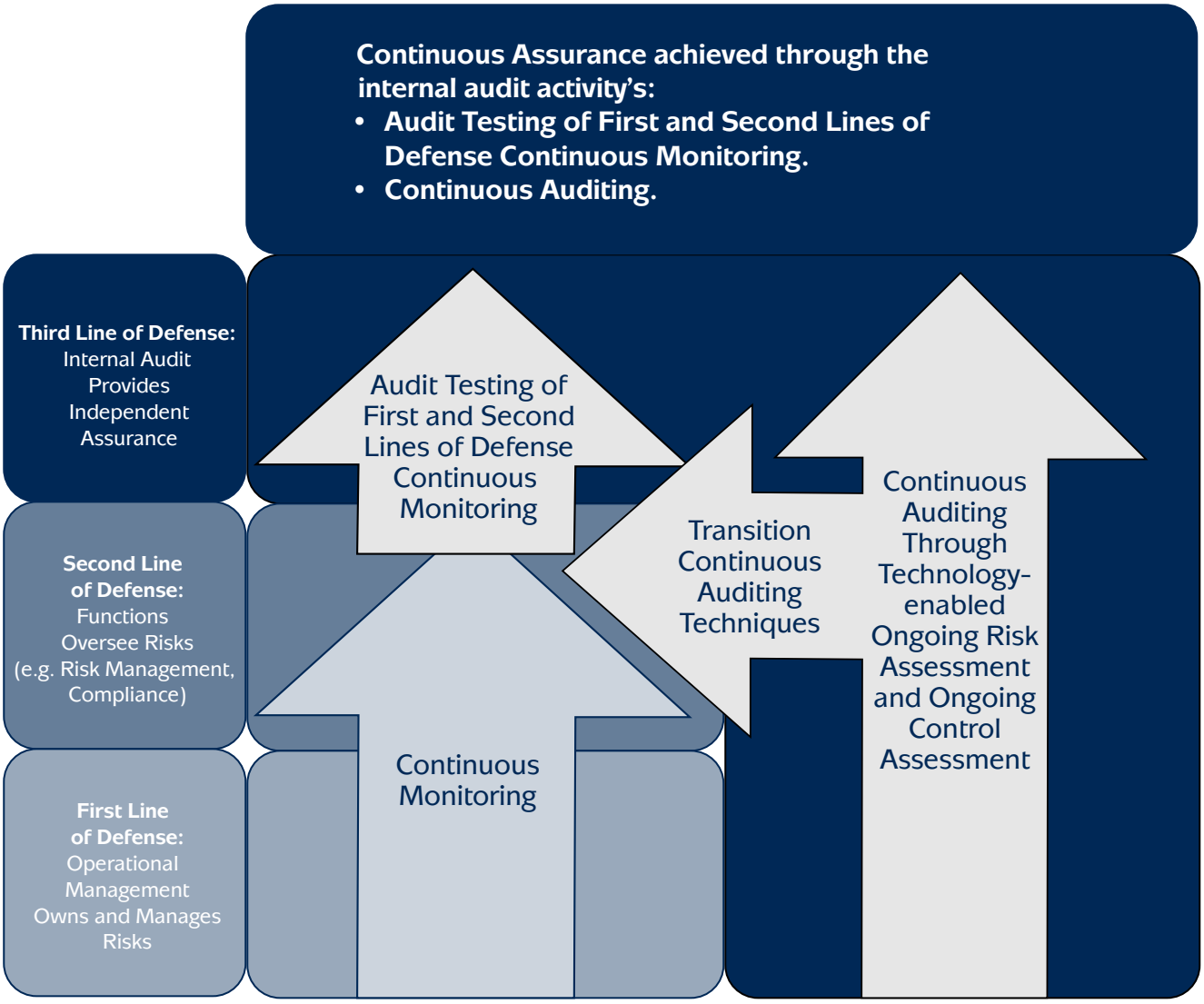
Used effectively, continuous monitoring can:

- Enhance the ability to promptly identify and curtail control problems.
- Reduce incidences of error and fraud.
- Enhance operational efficiency.
- Improve bottom-line results through a combination of cost savings and a reduction in overpayments and lost revenue.
- Improve customer satisfaction through enhanced customer service quality and integrity.

Optimized Continuous Assurance Framework

In some cases, internal auditors may strategically assist the functions that own and manage risks and controls (first line of defense) and the functions that oversee risks and controls (second line of defense) by helping to establish risk management and control processes. Continuous assurance is optimized when continuous auditing technology-enabled techniques are adopted for use in first and second lines of defense continuous monitoring efforts, and those continuous monitoring efforts are reliable and responsive to risk.

Figure 3: Optimized Continuous Assurance Framework

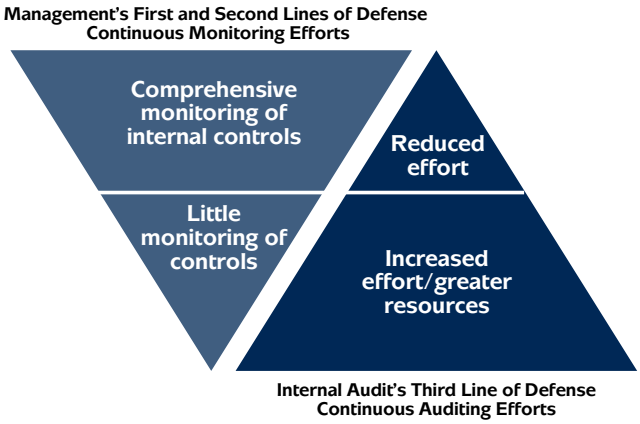


A fine line of distinction is introduced when continuous auditing techniques are adopted by management for continuous monitoring, because there is a potential for overlap between continuous monitoring and continuous auditing, and between the second and third lines of defense. When continuous auditing techniques are transitioned to management, care should be taken to ensure auditors do not assume an ownership role over continuous monitoring, which would presume to impair their objectivity.

Continuous Auditing/Continuous Monitoring Relationship

There is an inverse relationship between continuous auditing and continuous monitoring. All three lines of defense contribute to measuring and strengthening the effectiveness of risk management and control. Internal audit should adjust the extent of its continuous auditing work based on the adequacy and consistency of the continuous monitoring management deploys. If continuous monitoring deployed by the first and second lines of defense is lacking or inconsistent, internal audit should increase its continuous auditing efforts accordingly, as illustrated in Figure 4.

Figure 4:
Relationship Between Continuous Auditing and Continuous Monitoring Efforts



In areas where management has not implemented continuous monitoring, auditors should extend detailed testing using continuous auditing techniques. Where the first or second line of defense performs continuous monitoring on a comprehensive basis across end-to-end business process areas, internal audit may not need to perform the same detailed techniques as would otherwise be applied under continuous auditing. Instead, auditors should perform procedures to determine whether the continuous monitoring process is reliable. Such procedures include a:

- Review of detected anomalies and management's response.
- Review of management's resolve to enact and sustain remediation.
- Review and testing of controls over the continuous monitoring process itself, such as:
  - Security.
  - Change control.
  - IT operations.

These procedures are similar to IT general controls tests and diligence performed during the normal audit process to assess the reliability of CAATs.

Practical Applications for Continuous Auditing

Continuous auditing supports audit activities throughout the audit process. As illustrated in Figure 5, continuous auditing can be applied to audit plan development, audit engagement support, and audit recommendation follow-up. In addition, the CAE should recognize there are several second line of defense functions with strong links to continuous auditing such as risk management, compliance, ethics, and security. Internal audit should determine how continuous auditing can be leveraged to assess second line of defense functions and to use information generated by those functions.

Audit Plan Development

During the audit plan development phase, continuous auditing helps auditors to compile and sustain an audit universe that is more responsive to risk. Rather than scheduling audits according to a standard cycle of one-, two-, or three-year rotations, the frequency of audits should be based on risk, complexity, pervasiveness, and velocity of change. Continuous auditing helps internal audit quickly identify changes in risks and potential exposure.

Application of Ongoing Risk Assessment

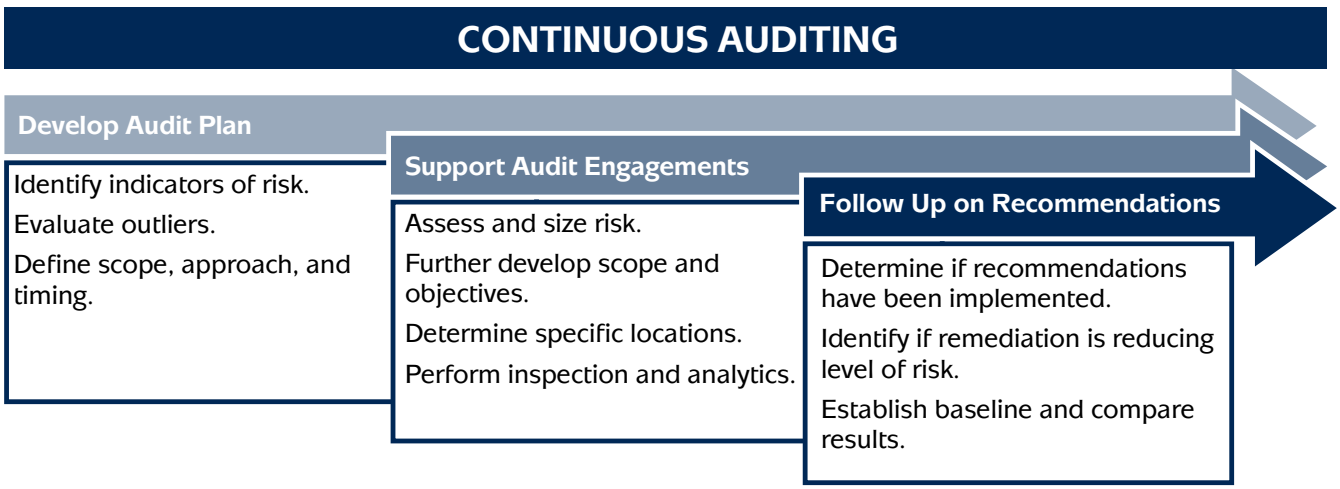
Data analytics should be used to support the development of leading indicators to trigger specific audits or areas to be included in the plan. For example, signaled by leading indicators, ongoing risk assessment can be leveraged in a large-scope audit to select locations to be visited, focus audit objectives and scope, include specific audits or entities in the annual audit plan, or trigger an immediate walk-through of an entity where the risk has increased significantly without an adequate explanation.

Examples of practical applications for ongoing risk assessment during audit plan development include:

- The application of a more strategic context to the development of audit plans and making ongoing adjustments to the plan when risk profiles change.
- The allocation of scarce, highly skilled audit resources to outlier areas that represent the greatest risk exposure for the organization.
- The assessment of management's risk mitigation activities.
- The development of areas of focus and strategic themes for the internal audit universe.
- The scope and objectives of individual audit engagements.

The primary difference between leveraging an ongoing risk assessment to develop an enterprise audit plan versus supporting an audit engagement is the detail level of required information. Summary-level information may be sufficient to identify outliers and redirect resources when developing the audit plan. Conversely, more detailed information will likely be required to identify risks and test controls to support the scope and objectives of an audit engagement.

Figure 5: Continuous Auditing Throughout the Audit Process



Audit Engagement Support

Continuous auditing can be integral to audit fieldwork, and continuous auditing techniques often improve and mature during the course of audit engagements. Auditors design and modify continuous auditing techniques as they discover risk drivers and evaluate audit analytics and remediation efforts. Continuous auditing enables auditors to:

- Refine the engagement scope to better focus on risk.
- Perform audit testing in situations where the audit objective cannot be accomplished by comparison data alone.
- Drill down to identify risk indicators and assess critical controls.
- Detect symptoms of fraud, waste, and abuse through the identification of anomalies and outliers.

Audit analytics and continuous auditing techniques differ with regard to scope, timing, and purpose.

- Audit analytics normally are:
  - Bound by the scope and timeline of a specific engagement.
  - Designed to improve the quality of an engagement.
- Continuous auditing techniques, often originating from analytics and lessons learned from prior audits, are conducted systematically and frequently during and beyond the scope and timeline of an audit engagement, and provide timely notification of trends, patterns, and outliers.

Application of Ongoing Risk Assessment

During an engagement, ongoing risk assessment can be used to better understand the business process. For example, in accounts payable (AP), examining payment types may lead to the discovery that electronic fund transfers are being completed by one AP office and that manual checks are being produced by another. This information allows the auditor to better understand the AP process at each location and assess the risk accordingly.

Application of Ongoing Control Assessments

Practical applications for ongoing control assessment during an audit engagement include:

- Examining transactional data (e.g., flagging all purchase card transactions that are greater than the authorization limit or that involve prohibited merchants).
- Evaluating configurations:
  - Interrogating systems to determine the condition of configurable automated controls.
  - Reviewing approval levels and access capabilities.
- Assessing program and parameter changes.
- Scanning incident and error management.
- Reviewing summarized data (e.g., where a cardholder's total monthly transactions are greater than US$10,000 and the cardholder is outside of the purchasing function).
- Employing comparative analysis (e.g., total overtime payments compared to all other employees in the same job classification, and threshold for identifying excessive or unauthorized overtime).
- Testing general ledger account balances (e.g., highlighting accounts where the balance differs by more than 25 percent compared to the previous year to identify unusual activity such as an increase in write-offs).
- Compliance testing for maintenance of current material safety data sheets for all substances purchased, stored, manufactured, or sold.

In all cases, auditors can quickly drill down into the details to evaluate the potential cause and perform required follow-up more promptly and potentially more easily.

Follow Up on Audit Findings

Application of Ongoing Risk Assessment

Leveraging ongoing risk assessment to follow up on audit findings is a powerful tool in ensuring continuous improvement and heightened performance. After an engagement, auditors can leverage ongoing risk assessment to determine if recommendations have been implemented and whether the remediation plans are having the desired effect.

Management's action plans should identify performance indicators to evaluate successful remediation. Performance indicators make it easier to establish a baseline and compare results before and after the implementation of the recommendation. Auditors should collaborate with management to find appropriate indicators that can, ideally, be measured systematically.

Continuous Auditing Implementation

Successful continuous auditing implementation requires leadership, change management, and a phased approach that initially addresses the most critical business systems. Although each organization is unique, there are some common activities that should be carefully planned and managed when developing and supporting continuous auditing (see Table 2).

Table 2: Key Steps to Implementing Continuous Auditing

KEY STEPS TO IMPLEMENTING CONTINUOUS AUDITING	
1. ESTABLISH A CONTINUOUS AUDITING STRATEGY • Coordinate with first and second lines of defense. • Set priorities and gain management support. • Adapt the annual audit plan to specify ongoing indicators.	
2. ACQUIRE DATA FOR ROUTINE USE • Establish routine access to the production environment. • Develop analysis capabilities. • Build audit technical skills and knowledge. • Assess reliability of data sources. • Prepare and validate the data.	
3. CONSTRUCT CONTINUOUS AUDITING INDICATORS	
ONGOING RISK ASSESSMENT • Develop risk indicators. • Design analytics to measure increased levels of risk.	**ONGOING CONTROL ASSESSMENT** • Relate to control objectives. • Determine key controls. • Evaluate baseline condition and changes to controls.
4. REPORT AND MANAGE RESULTS • Establish a repeatable methodology. • Report results. • Facilitate management action. • Align with continuous monitoring and adapt the continuous auditing strategy.	

The sequence of the activities in Table 2 may vary, and other activities not identified may need to be performed when developing continuous auditing to support a specific audit.

Establish a Continuous Auditing Strategy

The CAE should establish a short- and long-term continuous auditing strategy, with authority granted through an approved mandate, mission, or internal audit charter. For example, a short-term strategy might include the introduction of continuous auditing to support regulatory compliance audits. However, additional benefits in the form of improved business performance can be equally significant. Key activities are as follows.

Coordinate with First and Second Lines of Defense

Coordinate with first and second lines of defense to encourage business line and IT buy-in and support of the continuous auditing strategy. Internal audit should address the end-to-end business process and interdependent IT controls. 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. As such, ensuring reliability, integrity, and availability of business systems and data should be a key objective for the CAE and senior management. Continuous auditing can support the achievement of this objective by facilitating the assessment of risk management and control.

Set Priorities and Gain Management Support

Continuous auditing requires continual access to production applications and data. Reliable technologies may require significant investment and multi-year implementation efforts. Therefore, the support of the board and senior management is essential. A strategy that includes phased implementation over two or more years will help manage the pace and expectations, and steadily

show the benefits of continuous auditing technologies and methodologies.

Adapt the Audit Plan to Specify Ongoing Indicators

Develop a road map for mega-process areas such as procurement-to-pay or customer-to-cash, and then relate continuous auditing techniques to three related risk categories: IT operations, applications, and business process transactions. Leverage audit analytics to design specifications for risk and control indicators. Coordinate the internal audit plan to identify process areas and audits to specify key risk indicators (KRIs) and control measurements for use in subsequent ongoing assessment. Through scheduled audit engagements, audit teams and management can collaboratively consider leading and lagging indicators that measure risk and controls related to business objectives. Then, leverage the audit engagement results to develop forward-looking specifications (see Figure 6).

Acquire Data for Routine Use

Continuous auditing is not purely a technical issue. However, the selection of enabling technologies is essential to its long-term success. The continuous auditing strategy should guide the selection of software solutions. When selecting technologies for continuous auditing, the CAE should consider the technologies and capabilities in place in the organization's IT portfolio. It is important to connect the program with the organization's computing environment and future plans for key business systems. Audit-specific analytic software solutions provide flexibility and can read diverse data types, including mainframe legacy systems, client/server, and Internet-enabled systems, or enterprise resource applications such as SAP, Oracle, and other core business systems. See The IIA's GTAG 16: Data Analysis Technologies for more information. Key activities are described as follows.

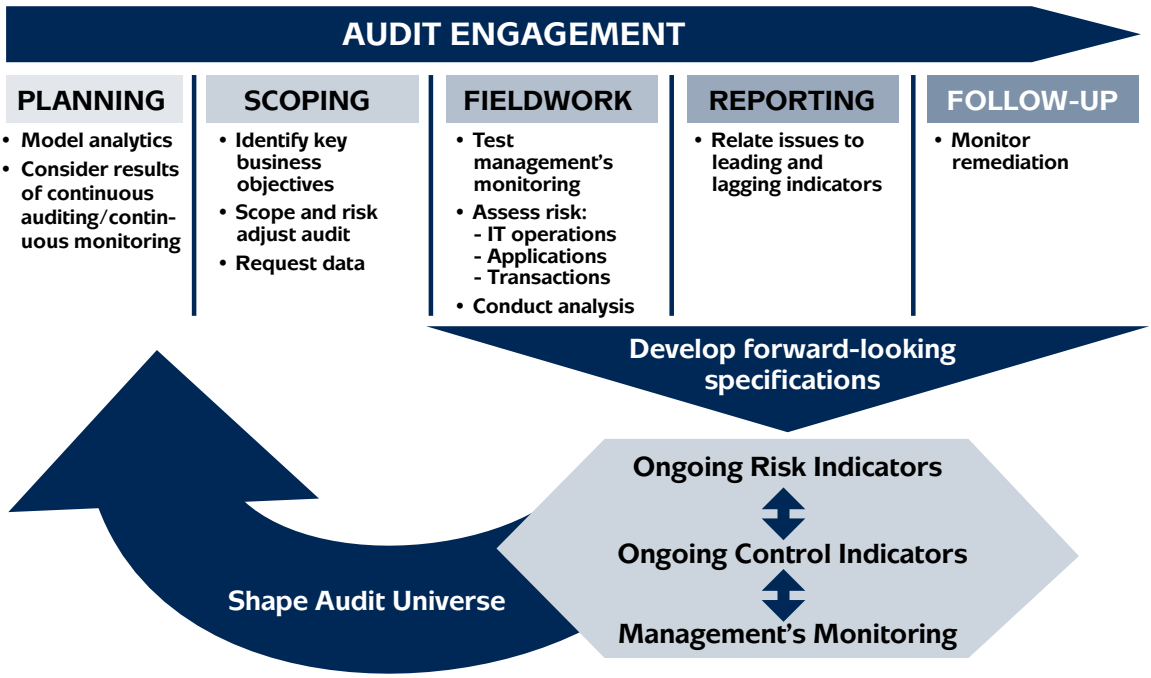
Establish Routine Access to the Production Environment

The CAE should work with management to affirm internal audit's access and use of business systems' data does not adversely affect the operational performance of the production environment and related systems, and that audit technology is compatible with the enterprise IT environment. Internal audit should assess applicable privacy regulations[3], and maintain privacy and security standards that meet or exceed those maintained in the production environment.

Develop Analysis Capabilities

Build analysis capabilities in accordance with the continuous auditing strategy and business objectives before automating monitoring. Continuous auditing evidence

Figure 6: Develop Forward-looking Specifications for Risk and Control Indicators



[3] For more information, see The IIA's Practice Guide, Auditing Privacy Risks.

often is sufficiently persuasive using a combination of indicators, such as changes to automated controls, system security, incidents, outliers, and transactions. Discussions with business system owners can help auditors determine the transfer method, schedule, and data protocol best suited for continuous auditing.

Build Audit Technical Skills and Knowledge

Standard 1210 requires that internal audit collectively possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities. Varying levels of IT proficiency will be required as continuous auditing is developed and implemented. For example, in the early stages of implementation:

- Parameter sensitivity, depth of analysis, and other factors may result in a high volume of flagged transactions. The workload required to discern the results will decrease as controls are improved, analytics are refined, and continuous auditing matures.
- Results may be prone to errors in data interpretation. Inaccuracies may be due to a lack of understanding and familiarity with the business systems and the nature of the tests being performed.

To enhance IT proficiency:

- Review key data fields and data elements.
- Review metadata created by functions applied to the data.
- Ascertain the timeliness of the data.
- Is the information current?
- How often is the information updated?
- When was the last update?
- Determine whether the information is complete and accurate.
- Verify the auditor's assumptions and analysis with the application programmers.
- Verify the integrity of the data by performing various tests such as reasonability, edit checks, and comparison to other sources, including previous investigations or audit reports (e.g., syntactic, semantic, and pragmatic data integrity).
- Leverage knowledge gained from internal audit engagements.

Assess Reliability of Data Sources

Data reliability is critical to successful continuous auditing implementation and should be assessed during a baseline audit. Data sourced from a production environment subject to IT general controls is more reliable than data sourced from end-user developed applications. As reliability increases, the level of testing and verification necessary to reduce audit risk to an acceptable level decreases. See GTAG 14: Auditing User-developed Applications for more information.

Prepare and Validate the Data

Develop a robust data validation capability and criteria to ensure integrity, previous to analysis. One of the greatest powers of continuous auditing is to extract data from a variety of systems across the organization and to relate it for further cross-platform analysis. Combining data from disparate systems requires data validation to remove unreliable transactions and prepare the data in a standard audit format. Automated data feeds can reduce validation time and increase the frequency of analysis.

Construct Continuous Auditing Indicators

Build a road map that is integrated with the audit plan. Design and construct the continuous auditing techniques based on learnings and specifications that resulted from previous traditional audits.

Ongoing Risk Assessment

Consistent with Standard 2120, continuous auditing enables auditors to "evaluate the effectiveness and contribute to the improvement of the risk management processes." Key activities and considerations in performing an ongoing risk assessment include:

- Develop risk indicators:
  - The collection and analysis of data supporting key business processes and high-risk areas should be gathered from multiple levels of the organization to identify, assess, and respond to risks.
  - Collaborate with business owners and IT professionals to develop risk indicators that are easily measurable and are sensitive to change.
  - Leverage risk assessment results to potentially modify the audit plan, as well as individual audit scope and objectives.
- Design analytics to measure increased levels of risk.
  - KRIs should:
    - Focus on the extent of change experienced by the entity over time (design KRIs to facilitate trending).
    - Be a combination of process-based leading indicators and symptomatic lagging indicators.
    - Be identified in sufficient number that when routinely compared will isolate outlier entities that are accepting risk beyond the established risk tolerance level.

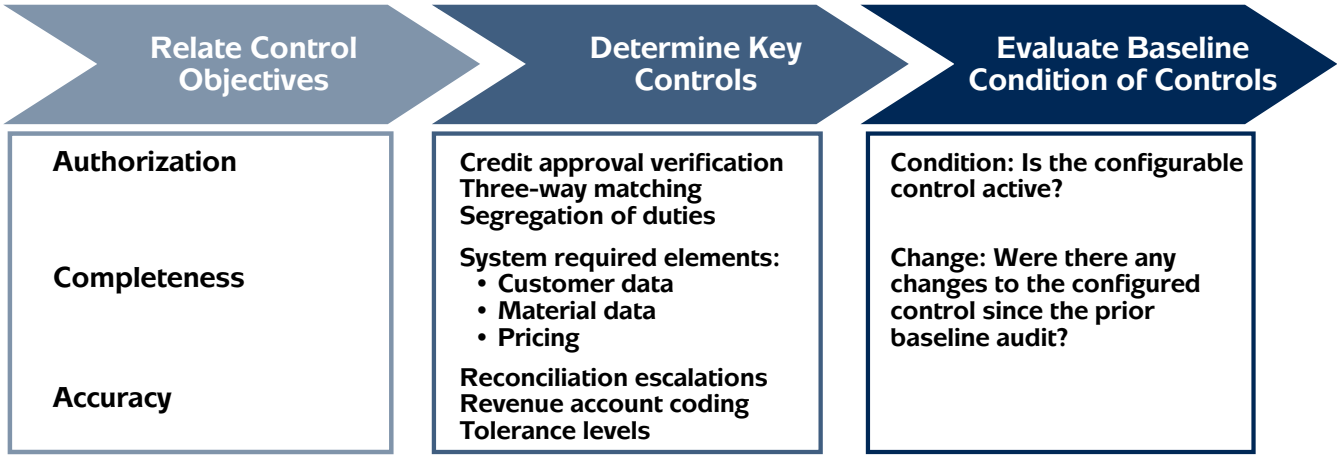
Ongoing Control Assessment

An ongoing control assessment provides independent analysis of automated application controls and IT general controls by evaluating their baseline conditions and subsequent changes to configuration. Because degradation of IT controls often occurs in advance of symptomatic errors in data, the use of ongoing control assessment enables the CAE to provide management with an early warning of control violations or deficiencies. Key activities and considerations in performing an ongoing control assessment include:

- Relate to control objectives.
  - Guard against the tendency to automate each step of an existing audit program. Rather, identify a smaller number of analytics that relate to high-level control objectives.
  - The true power of ongoing control assessment lies in the ability to provide relevant assurance effectively and timely.
  - Because IT general controls enable the ongoing reliability of automated controls, evaluating IT general controls and automated application controls is integral to optimizing the assurance and compliance process.
  - Automated controls are configured in applications to enforce the accuracy, completeness, and authorization of transactions. Gain an understanding of automated controls through joint discussions with management and technology experts.
- Determine key controls.
  - Walk through a business scenario and consider what could go wrong. Determine how automated techniques have been designed and configured in the system to control authorization, completeness, and accuracy of transactions.
  - Interrogate configured controls systematically to determine their current and baseline conditions and evaluate whether they are operating effectively as designed.
  - Monitor changes, which should be infrequent, to automated, configurable controls. Automated controls that are not configured well or change frequently decrease the auditor's confidence in the effectiveness of control activities.
- Evaluate the baseline condition of controls.
  - Once key business processes, related control objectives, and automated controls are defined, rank them to identify critical control points (highest impact/risk).
  - For critical control points, define appropriate analytics for each control objective.
  - Evaluate the current condition of configured automated controls as compared to a baseline value.
  - Determine if the condition of the configured automated control has changed since the prior baseline audit.
  - Consider the frequency and extent of changes to configured automated controls.
  - Align transaction exceptions to corroborate effectiveness.

As an example, Figure 7 describes an ongoing control assessment for a customer-to-cash business process.

Figure 7: Customer-to-cash Ongoing Control Assesssment



Report and Manage Results

After designing and constructing continuous auditing indicators, internal audit should schedule ongoing risk and control assessments in connection with the audit universe. Ongoing assessments should analyze the results of the continuous auditing techniques, probe as necessary, and report recommendations.

Deliverables can range from a straightforward graphic of comparisons and trends to data visualization of risk and control (see the appendix). The process is iterative and competence in continuous auditing/continuous monitoring grows as auditors collaborate with the first and second lines of defense. Successful continuous auditing/continuous monitoring programs promote timely decision-making, coordinated action plans, and successful issue remediation.

Establish a Repeatable Methodology

A structured methodology for managing results should include these steps to ensure that exceptions identified are addressed and remediated timely:

1. Review and discern exceptions to measure risk with increasing accuracy.
2. Perform root cause analysis to identify control weaknesses in design, execution, or both. Addressing root cause conditions can deter recurrent exceptions, lead to better recommendations, and highlight the value-add of continuous auditing methodology.
3. Develop a recommendation for remediation.
4. Record and track management's action plan for remediation.

Report Results

It is preferable to report continuous auditing results through a website rather than sending large, sensitive files via email. Reporting strategies range from simply exporting exceptions into a shared folder on a network drive, to email notifications, workflow remediation tracking, dashboards, and data visualization. A variety of reporting solutions may be implemented to meet the needs of the first, second, and third lines of defense, management, and the board. Key considerations for reporting continuous auditing results include:

- Regularly publishing a comprehensive set of reports to a network drive at the level of detail required to support continuous monitoring and continuous auditing.
- Storing exception results in a secure database.
- Presenting trending information in a Web-based dashboard or heat map.

Facilitate Management Action

Each action plan should have an owner responsible for remediation through to resolution. The exception should be delineated and reported as resolved, and subsequent continuous monitoring should measure how well the remediation is sustained.

Align with Continuous Monitoring and Adapt the Continuous Auditing Strategy

Continuous auditing should remain flexible and responsive to changes in risk exposure and the control environment. The CAE should periodically refresh the continuous auditing program strategy to adapt to new priorities and themes. Additional control points or risk exposures may need to be added, and others may be transitioned to management's continuous monitoring efforts. Over time, thresholds and control tests and parameters for various analytics may need to be tightened or relaxed. Subsequent to implementation, the CAE should record the benefits realized by continuous monitoring in other management initiatives such as enterprisewide risk management and performance measurement. Quantifying the benefits experienced by auditors and other assurance providers documents return on investment, enhances reputation, and justifies funding for further investment and strategic development.

Appendix – Case Studies

This appendix illustrates three practical applications of continuous auditing.

- Case A.1 Ongoing Control Assessment of Application Controls
- Case A.2 Ongoing Control Assessment of an Employee Expense System
- Case A.3 Ongoing Risk Assessment of a Manual Journal Voucher Process

A.1 — Ongoing Control Assessment of Application Controls

Application controls are configured to enforce the completeness, accuracy, and authorization of transactions. Automating the review of application controls can help auditors and compliance professionals answer these questions:

- How often do changes occur to automated controls?
- Did the application or IT team apply any upgrades or patches?
- Has the configuration of any major business process been modified?
- Could any of the changes impact the way the application behaves?

Answers to these questions can determine the need for further testing and potentially increase audit efficiency and effectiveness.

In this case study, an ongoing assessment of application controls was linked to a reduction in control testing labor by nearly 6,000 working hours compared to the previous year. After gaining the support of key stakeholders such as management, IT, external auditors, and application owners, internal auditors identified key objects of the control configuration, automated data extraction, and benchmarked results.

Identify the Key Objects of the Control Configuration

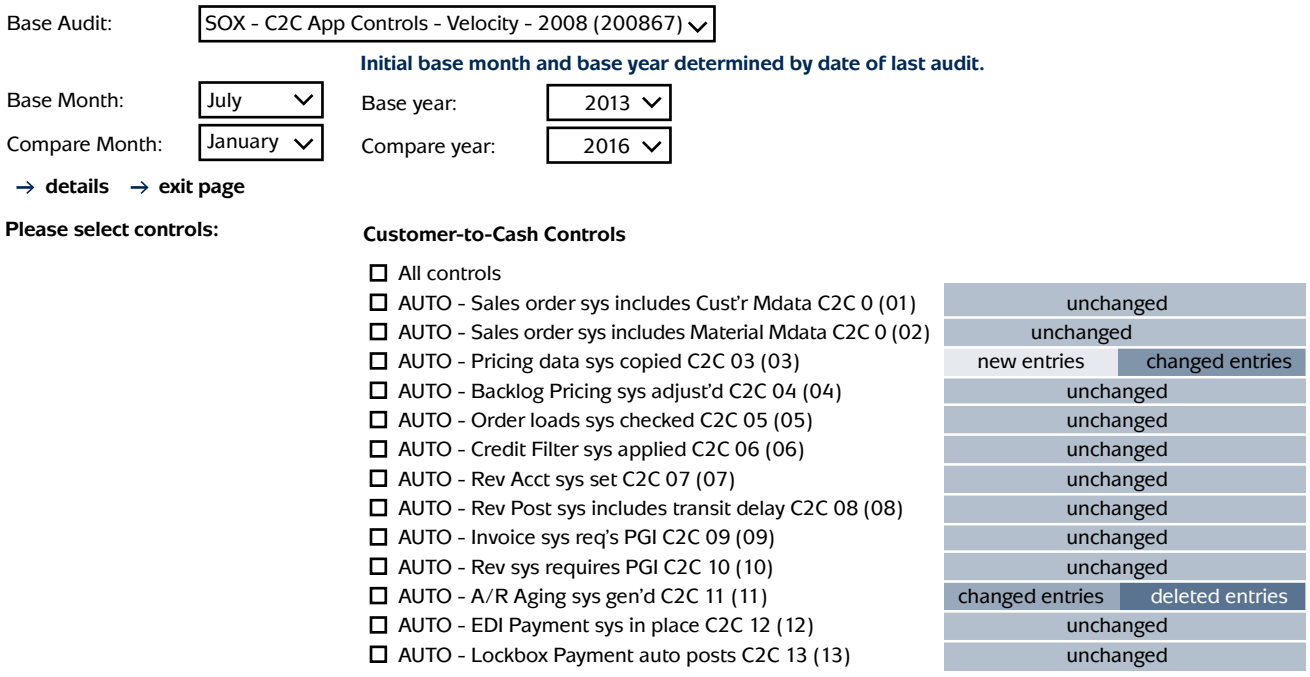
The first step toward ongoing control assessment was to identify the key objects within the application control function, including programs, screens, Web pages, and tables. The next steps were to determine how to automate data extraction and whether the controls were changed.

Automate Data Extraction of the Application

A variety of commercial data extraction tools are available. However, in this case, a data extraction tool developed in-house was readily available, reducing the cost of continuous auditing implementation. Once the tool was selected, certain decisions needed to be made:

- How often should the control data be pulled from the application for comparison to the baseline?

Figure 8: Application Controls – Benchmark Report



- Who should maintain the data history and where will it be stored?
- When comparing control data to the previous baseline audit, who should be responsible for assessing the significance of the changes in the application and determining which controls need to be retested?

Benchmark Results

After the data was extracted, it was compared with a base period. The benchmark report identified the key automated controls that were subjected to change since the base period, and the type of change (see Figure 8 on page 16). Ideally, application controls should be unchanged.

Auditors selected key controls and drilled down to assess the change. As appropriate, benchmark reports were incorporated into the audit workpapers, either to provide evidence that further control testing was not necessary or to support the need for retesting. In this way, benchmarking facilitated a risk-based approach to retesting, which was performed through management's continuous monitoring efforts when possible, providing additional efficiency.

After implementation of the ongoing control assessment, 58 percent of application controls could be validated without testing. Of the remaining 42 percent, 16 percent were tested during the first half of the year, and 26 percent were retested during the second half of the year. Time required for application control testing fell from 6,300 to 352 working hours, a 94 percent decrease year-over-year (see Figure 9).

A.2 — Ongoing Control Assessment of an Employee Expense System

Continuous auditing potentially is most effective when applied to high volume systems accessed by a large number of users. This case illustrates how internal auditors applied continuous auditing techniques to an employee expense system audit.

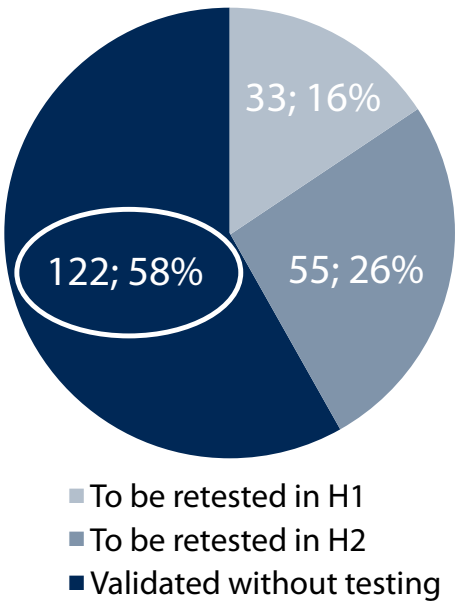
Background and Challenges

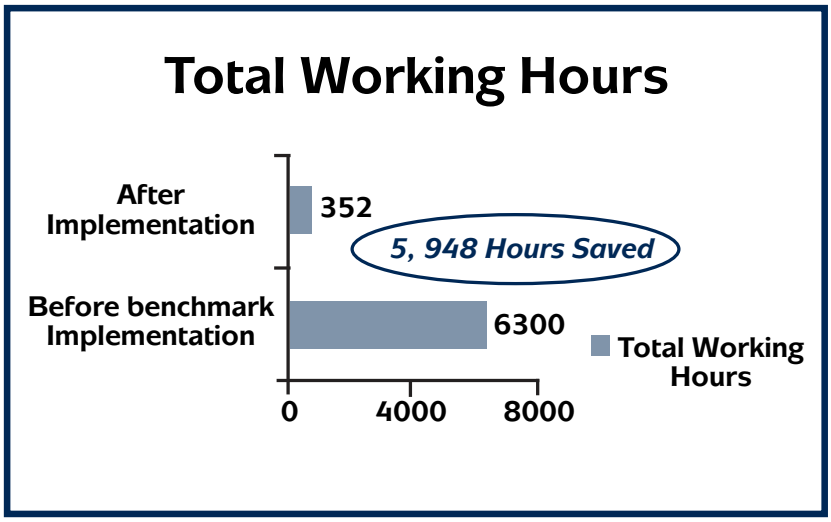
Previous audits of the employee expense systems were time consuming and labor intensive, and the audit scope was sometimes limited by resource constraints. The employee expense system was rules-based with numerous automated controls implemented at multiple levels to manage the quality of data entered and initiate the expense approval process. Examples include:

- An expense submission control:
  - If duplicate expenses were entered for the same date, category, and amount, the system would give the user a warning, require a manager's active approval, and flag the entry for operation's review.
- Active approval controls:
  - At-risk transactions were held pending a supervisor's review.
  - An employee could not approve his or her own report.

Controls were typically focused on limits or authorizations but did not necessarily check the validity or accuracy of the data entered. Inadvertent or intentionally incorrect

Figure 9: Total Working Hours Saved





categorization or misleading comments entered by an employee could go undetected. The effectiveness of the rules-based system was dependent upon:

- The accuracy and honesty of the employee entering the expense item.
- The willingness and ability of managers to accurately review and approve or deny the expense timely.

Faced with these challenges, the internal auditors tried to find the best way to test the validity of expense transactions.

The Continuous Auditing Solution

In summary, internal auditors determined:

1. Credit card transaction detail was available from the card issuer, and comparing the electronic expense system data with the card issuer's data could provide a better picture of the validity of the expenses.
2. Once the card issuer report data was matched with the electronic expense system data by employee number, charge date, and charge amount, the expense categorization and comments could be compared to the transaction merchant code and transaction description. For example, a transaction with a merchant code for a shoe store, but categorized in the expense record as a meal, could be identified.
3. The card issuer provided "questionable reports" that could be customized to target specific merchant classes and run on a monthly or quarterly schedule.

Following are examples of continuous auditing techniques that were used to identify control deficiencies, anomalies, and red flags indicating potential fraud and abuse. Although not quantified here, internal auditors reportedly reduced the hours previously needed to acquire data, perform data analysis, and vet and review results, compared to previous electronic expense system audits.

Questionable Spending Metrics

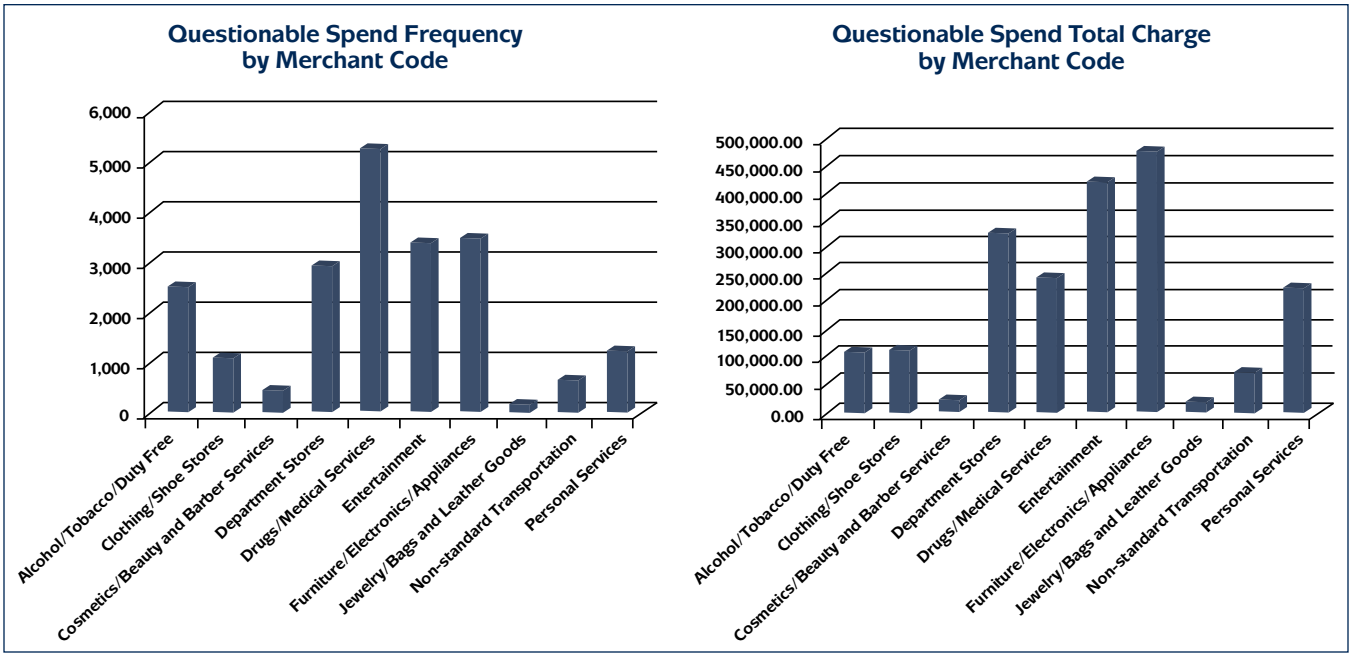
Identification of all questionable spending summarized by merchant code, employee, and establishment.

Questionable Spending at Restricted Establishments

Identification of all expense activity for restricted establishments billed back as an employee expense. Restricted establishments were identified by indicators such as legal supplier names, address match, sites with a mix of expensed and personal activity, split high dollar transactions, and restricted keywords (e.g., kids, hospital, nightclub, gentleman, casino, premium, and upgrade).

Incorrect Categorization Summary

Identification of all non-meal expenses (e.g., clothing expense) incorrectly categorized as a meal or entertainment.



Restricted Items

Identification of restricted keywords (e.g., kids, hospital, nightclub, gentleman, casino, premium, and upgrade) in the transaction description fields. This type of analysis typically requires the use of data analysis software.

Prohibited Word	Transaction Description 1	Transaction Description 2	Employee ID	Charge Date	Amount USD
KIDS	KIDS TOON AMMAN JORDAN AMMAN	23.000 JO DINAR CONVERTED TO	12345678	2015-01-12	32.49
HOSPITAL	AL KINDI SPECIALIZED HOSPITAL WLL MANAMA	5,000 BH DINAR CONVERTED TO	34567891	2015-01-22	13.26
NIGHTCLUB	BC OF NOLA 274600029 NEW ORLEANS LA	REF# ID6155 BAR/ NIGHTCLUB 15/01/15	23456789	2015-01-12	225.00

Top Expenses Without Receipt

Identification of the top dollar expenses within each expense category, submitted without a receipt.

Card Activity in Home City

Identification of continued card activity in and around the cardholder's billing address or city.

Hotel Folio

Identification of all hotel folio questionable spending summarized by item, employee, and hotel. This included items not reimbursed under the expense policy that were hidden within the total hotel charge.

Airline Fees

Identification of all air travel expenses where there was a mismatch between the expense comment/category and the supplier fee description. For example, items such as seat or cabin upgrades entered as an air or bag fee.

Personal Card Activity on Delinquent Cards

Identification of continued personal card activity on previously delinquent accounts.

Personal and Non-expensed Activity

Identification of all personal and non-expensed card activity compared to expense cash claims.

Split Expenses

Identification of expenses that might have been split to bypass transaction thresholds. This analysis was performed by looking for transactions with the same vendor and charge date. Data analysis tools with built-in functionality to analyze duplicates were found to be very helpful.

Employee ID	Supplier_No	Supplier_Name	Merchant Code	Charge Date	Amount USD
12345678	9945845279	EL ARRIERO STEAKHOUSE	EATING PLACES/RESTAURANTS	2015-02-11	450.00
12345678	9945845279	EL ARRIERO STEAKHOUSE	EATING PLACES/RESTAURANTS	2015-02-11	300.00
23456789	9903904407	WORLD CAR SA	AUTO RENTAL - ALL TYPES	2015-02-13	225.00
23456789	9903904407	WORLD CAR SA	AUTO RENTAL - ALL TYPES	2015-02-13	175.00

A.3 — Ongoing Risk Assessment of a Manual Journal Voucher (MJV) Process

An ongoing process-level risk assessment can:

- Identify new and emerging risks within a short time from the associated initial transaction.
- Help auditors identify abnormal trends and assess cumulative impact and the total value at risk.

This case highlights steps taken by internal auditors to develop and implement an ongoing MJV process risk assessment.

1. Understand the Process

The first step in developing the ongoing risk assessment was to develop a thorough understanding of the process. In this case, auditors conducted external research and gathered relevant information from management and process owners to gain an understanding of the total population, available reports, nonstandard areas, and dependencies on other processes. The next step was to build a prototype database of risk attributes that could impact the MJV process.

2. Create a Prototype Risk Database

Analytical and statistical tools were leveraged to create a prototype risk database. The database was developed through an iterative process that checked for data integrity, completeness, and logic accuracy. For example, the risk attributes of the MJV risk database included:

Risk Outcomes

- MJV impact on net profit.
- MJV impact on revenue and expenses.
- MJV impact on cash and other assets.
- MJV impact on liabilities.

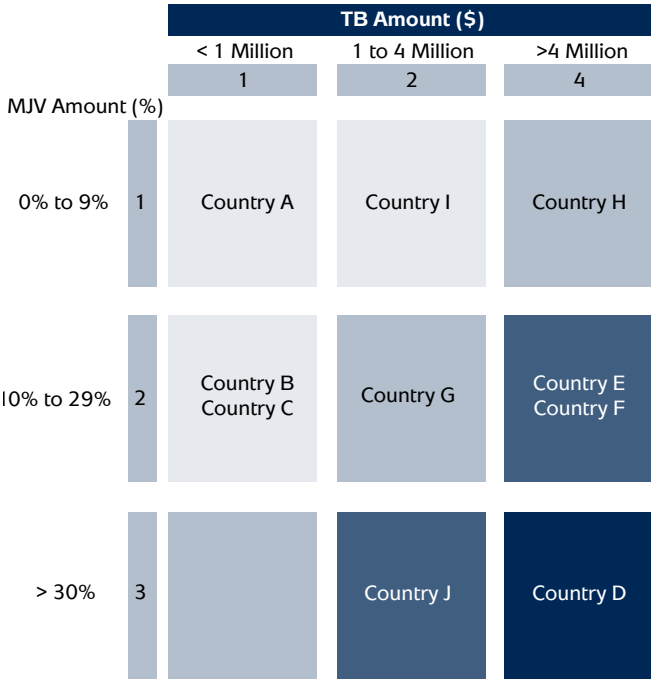
Risk Indicators

- MJVs posted by terminated users or unauthorized users.
- MJVs posted after cut-off date.
- MJVs posted on holidays.
- MJVs posted without adequate segregation of duties.
- MJVs posted without documentation or approvals.
- High value MJVs.
- Split transaction MJVs.

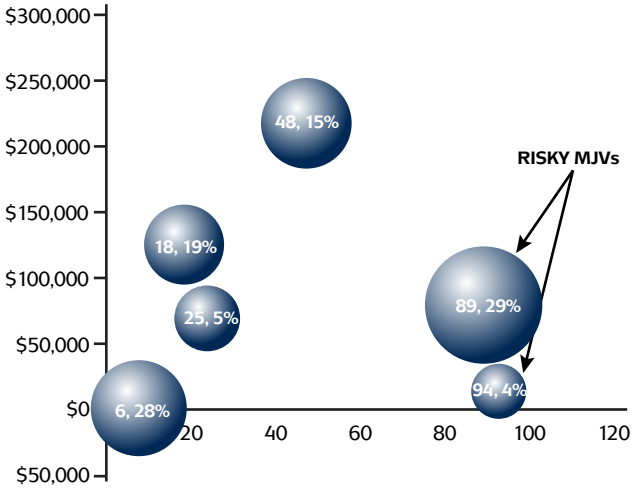
3. Identify Unknown Risks and Outliers Using Statistical Techniques

Statistical techniques were applied to identify new and emerging risks, potentially reducing the element of surprise. Grid, cluster, Benford's Law, regression, and what-if analyses were performed.

- Grid analysis was used to segment the population by two independent variables, MJV% and trial balance dollars (TB$). In the grid below, 10 countries were segmented to show the riskiest countries at a glance, as well as the best performing countries, which were tapped to share best practices.

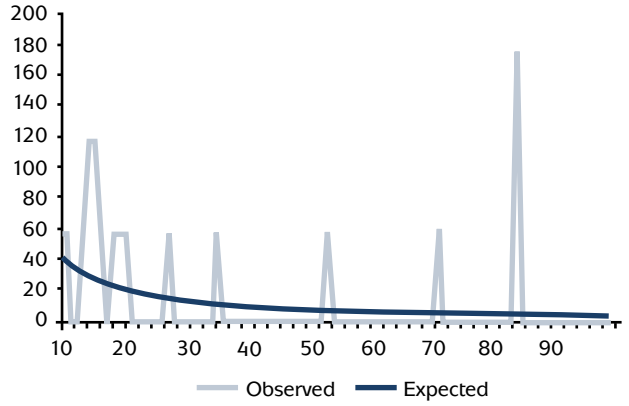


- Cluster analysis was used to segment the population and identify clusters of risky transactions using multiple variables such as high-dollar value, holiday postings, and year-end transactions.

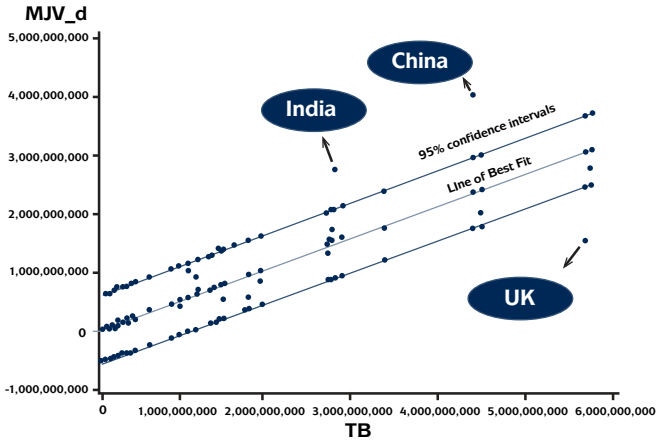


- Benford's Law was used to analyze the occurrence of certain digits within key numeric fields to find

abnormal, fabricated, or potentially fraudulent patterns. An example of an abnormal trend analysis for one country is below.



- Regression analysis was used to identify outliers. In the example below, regression analysis identified outlier countries using the total value of the MJV over the trial balance.



- What-if analyses were used to predict future relationships between variables.

4. Collaborate on Reporting Efforts

The ongoing risk assessment was designed to automatically populate outputs into graphs, tables, and other visuals for audit reports and dashboards. Audit dashboards were created systematically and then the process was expanded to include management dashboards. This avoided duplication of data and efforts required to generate reports and publish results for management. Management was better able to monitor key performance indicators. Collaboration helped internal auditors understand management's continuous monitoring results. Internal audit took care to maintain its independence and not take ownership of risks. Continuous monitoring reports informed management's action plans and provided enhanced opportunities to deter fraud and avoid surprises.

Authors, Reviewers, and Contributors

Authors:

Bradley C. Ames, CPA, CRMA, CISA
Roy D'Cunha, ACMA, CIA, CISA, CGMA
Patricia Geugelin-Dannegger
Peter B. Millar
Sajay Rai, CPA, CISSP, CISM
Andrew Robertson, CRMA
Thomas Steeves, CISA

Reviewers and Contributors:

David Coderre
Carrie Gilstrap, CISA
Steven Hunt, CBM, CGEIT, CIA, CISA, CRISC, CRMA
Steven E. Jameson, CIA, CCSA, CFSA, CRMA
Peter Schraeder
Dragon Tai, CIA, CISA, CCSA, CRMA
Jaroslaw B. Tarbaj, CISA

GTAG®

About the Institute

Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs, Fla., USA. The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator.

About Practice Guides

Practice Guides provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. Practice Guides are part of The IIA's IPPF. As part of the Strongly Recommended category of guidance, compliance is not mandatory, but it is strongly recommended, and the guidance is endorsed by The IIA through formal review and approval processes.

A Global Technologies Audit Guide (GTAG) is a type of Practice Guide that is written in straightforward business language to address a timely issue related to information technology management, control, or security.

For other authoritative guidance materials provided by The IIA, please visit our website at www.globaliia.org/standards-guidance.

Disclaimer

Copyright

The Institute of Internal Auditors

www.globaliia.org

140578