Continuous Auditing and Monitoring

3rd Edition

Global Practice Guide

Aligns with the Global Internal Audit Standards

The Institute of Internal Auditors

GLOBAL TECHNOLOGY AUDIT GUIDE

Acknowledgements

Global Guidance Council Reviewers (3rd Edition)

Nur Hayati Baharuddin, CIA, CRMA, CCSA, CFSA, CGAP, Malaysia

Ruxandra Bilius, CIA, CRMA, Romania

Gaston Lariau, CIA, CRMA, Uruguay

International Internal Audit Standards Board Reviewers (3rd Edition)

W. Charles Johnson, CIA, CRMA, QIAL, CFSA, CGAP, United States

Hans-Peter Lerchner, CIA, CRMA, Austria

IIA Standards and Guidance

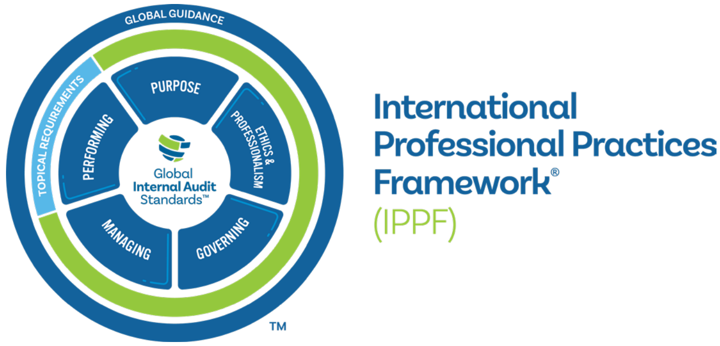
Benito Ybarra, CIA, CFE, CISA, CCEP, Executive Vice President

Katleen Seeuws, CIA, CRMA, CGAP, CFE, CISA, Vice President

William Truett, CIA, CISA, Senior Manager (Project Lead)

The IIA thanks the following oversight bodies for their support: Global Guidance Council, International Internal Audit Standards Board, and the International Professional Practices Framework Oversight Council. To learn more about contributing to Global Guidance, visit https://www.theiia.org/en/about-us/get-involved/volunteer-your-time/.

About the IPPF



A framework provides a structural blueprint and coherent system that facilitates the consistent development, interpretation, and application of a body of knowledge useful to a discipline or profession. The International Professional Practices Framework® (IPPF)® organizes the authoritative body of knowledge, promulgated by The Institute of Internal Auditors, for the professional practice of internal auditing. The IPPF includes Global Internal Audit Standards™, Topical Requirements, and Global Guidance.

The IPPF addresses current internal audit practices while enabling practitioners and stakeholders globally to be flexible and responsive to ongoing needs for high-quality internal auditing in diverse environments and organizations of different purposes, sizes, and structures.

Global Guidance

Global Guidance supports the Standards by providing nonmandatory information, advice, and best practices for performing internal audit services. It is endorsed by The IIA through formal review and approval processes.

Global Guidance provides detailed approaches, step-by-step processes, and examples on subjects including:

- Assurance and advisory services.
- Engagement planning, performance, and communication.
- Financial services.
- Fraud and other pervasive risks.
- Strategy and management of the internal audit function.
- Public sector.
- Sustainability.
- Global Technology Audit Guides® (GTAG®) provide auditors with the knowledge to perform assurance and advisory services related to an organization's information technology and information security risks and controls.

Global Guidance is available as a benefit of membership in The IIA.

Contents

Executive Summary

Rapidly changing global business conditions have created an opportunity for organizations to develop continuous auditing programs for financial and operational data. Such programs support the internal audit function's ability to provide the board and senior management with continuous assurance of effective risk management and control processes.

Continuous auditing comprises ongoing assessments of risks and controls, enabled by technology and facilitated by a new audit paradigm that has shifted from periodic evaluations of risks and controls based on a sample of transactions to ongoing evaluations based on larger samples of transactions.

Internal auditors can use technology such as artificial intelligence to create algorithms for analyzing vast datasets in real time, detecting anomalies and trends that may signal risks or control weaknesses. Auditors can also use natural language processing to process and understand unstructured data, providing a more comprehensive view of the organization's activities.

Continuous monitoring is an ongoing management process of reviewing whether controls operate effectively. Integrating continuous auditing programs with operational management's continuous monitoring initiatives can increase efficiency and maximize insights.

This guide supersedes "Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance, 2nd Edition," published in 2015.

Introduction

The **internal audit function**'s typical approach to evaluating the effectiveness of **risk management** and control processes is often retrospective, with **controls** tested on a cyclical basis, perhaps months after business activities have occurred. Two factors are driving the internal audit function's efforts to modify this approach:

- The organization's desire to keep pace with the business by responding in a timely manner to accelerated rates of change and emerging **risks**, particularly from a technological standpoint.
- Advancements in technology such as **artificial intelligence** and **natural language processing** have enabled both ongoing **risk assessments** and ongoing control assessments.

There are five key steps to implement continuous auditing:

1. Establishing a continuous auditing strategy.
2. Identifying potential technology solutions.
3. Acquiring data for routine use.
4. Constructing continuous auditing indicators (ongoing assessments and risks controls).
5. Reporting and managing the results of internal audit services.

Continuous auditing also includes analyzing data sources that can reveal anomalies in business systems, such as security levels, **incident** logging, unstructured data (data that is not restricted to a fixed field in a spreadsheet or database), and changes to IT **configurations**, **application** controls, and segregation-of-duty controls.

For organizations that follow The IIA's Three Lines Model, the first line comprises operational management functions that own and manage risks by establishing and implementing controls. The second line includes management functions such as **compliance** and enterprise risk management departments that monitor and challenge risk-related matters. The third line is the

Note

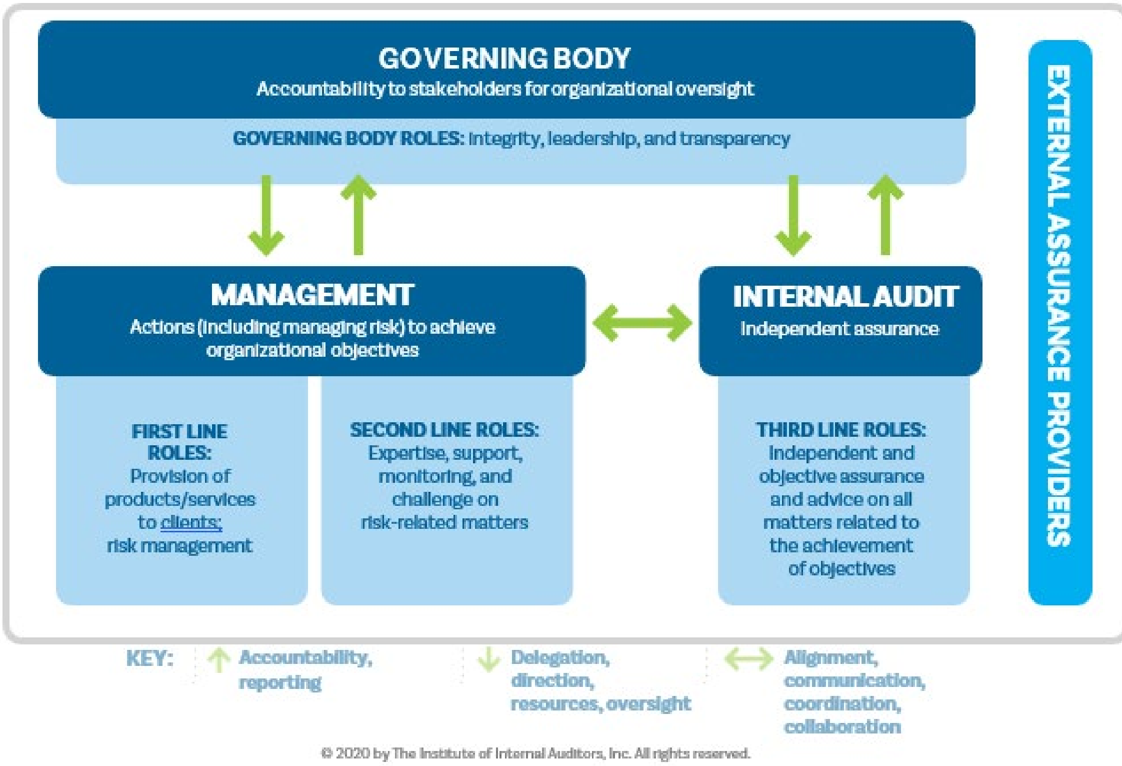
Terms in **bold** are defined in the glossary in Appendix B.

The Global Internal Audit Standards use certain terms as defined in the glossary. To understand and implement the Standards correctly, it is necessary to understand and adopt the specific meanings and usage of the terms as described in the glossary.

The Standards use the word "must" in the Requirements sections and the words "should" and "may" to specify common and preferred practices in the Considerations for Implementation sections.

internal audit function, which provides independent and objective **assurance** over the effectiveness of **governance,** risk management, and **control processes**.

Figure 1. The IIA's Three Lines Model



Continuous monitoring encompasses ongoing efforts by the first and second lines 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. The internal audit function can provide the organization with continuous assurance by performing ongoing testing of continuous monitoring concurrently with its continuous auditing activities.

Continuous auditing can help with developing the **internal audit plan** (Standard 9.4 Internal Audit Plan), supporting the internal audit **engagement** (Standard 10.3 Technological Resources), and following up to ensure internal audit **findings** are resolved (Standard 15.2 Confirming the Implementation of Recommendations or Action Plans).

Chief audit executives should be aware that continuous auditing will change the nature of evidence, timing, procedures, and level of effort required by internal auditors (Standards 3.1 Competency, 4.2 Due Professional Care, and 10.2 Human Resources Management). Coordinating continuous monitoring, continuous auditing, and audit testing of continuous monitoring helps the **internal audit function** and management generate value, achieve strategic and operational goals, and enhance the organization's ability to create, protect, and sustain value. (Standards 9.5 Coordination and Reliance and 14.4 Recommendations and Action Plans).

A coordinated effort results in the timely notification of gaps and weaknesses in risk management and control processes, creating an opportunity to improve follow-up and corrective action (Standard 15.2 Confirming the Implementation of Recommendations or Action Plans). Coordinating the organization's continuous auditing and continuous monitoring efforts can improve overall organizational understanding of data, risk, and control and maximize the internal audit function's ability to provide the **board** and **senior management** with effective continuous assurance and monitoring.

Business Significance

In many organizations, the board and senior management show signs of fatigue from actual or perceived duplication or overlap of reviews of risk management and controls among the three lines. Continuous auditing may help mitigate this fatigue by:

- Optimizing the balance between the review efforts of the internal audit function and management (Standard 9.5 Coordination and Reliance).
- Promoting more efficient use of organizational resources.
- Reducing the cost of assessing and providing assurance over the adequacy of controls.
- Providing ongoing evaluation of risks and controls.
- Providing timely reporting of gaps and weaknesses, enhancing the opportunity for prompt corrective action.
- Providing the flexibility necessary to prioritize remediation.
- Promoting better understanding of business performance, risks, and compliance.
- Enabling the internal audit function to provide continuous assurance regarding risks, controls, and improvement opportunities.

Roles and Responsibilities

The performance and coordination of continuous auditing and continuous monitoring to provide continuous assurance requires a clear understanding of roles and responsibilities.

Figure 2. Continuous Assurance Roles and Responsibilities

Role	Responsibilities
Chief audit executive	• Establish credibility for continuous auditing activities by ensuring the capability of internal auditors (Standards 3.1 Competency and 3.2 Continuing Professional Development) and the sufficiency of their tools, data security arrangements, and budget (Standards 10.1 Financial Resource Management, 10.3 Technological Resources, and 13.5 Engagement Resources). • Educate internal auditors, senior management, and the board on the roles and responsibilities of the internal audit function and management. • Commit to a multiyear strategy to encourage support from **stakeholders** (Standards 6.3 Board and Senior Management Support and 9.2 Internal Audit Strategy). • Communicate the results of the internal audit function's assessment of the effectiveness of continuous monitoring (Standards 11.3 Communicating Results and 15.1 Final Engagement Communication).

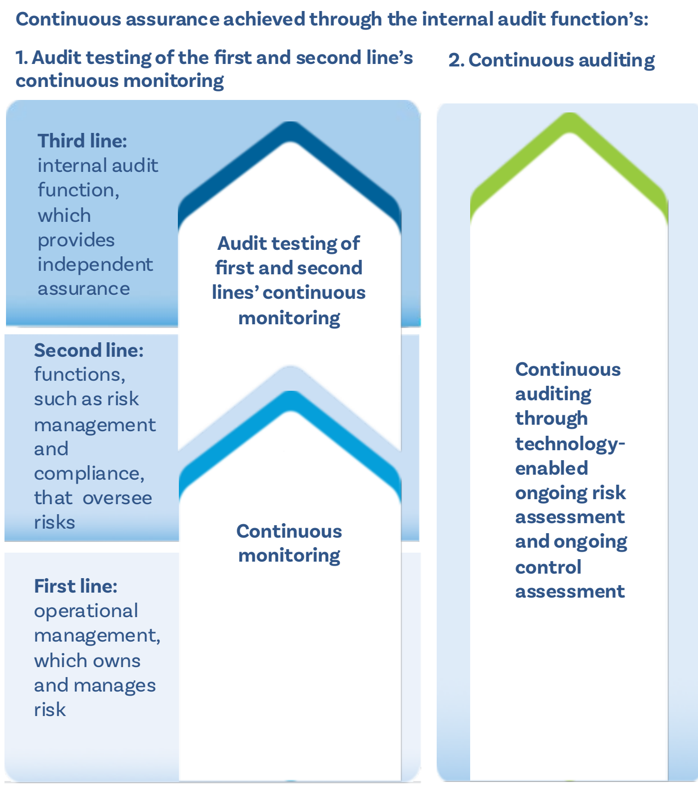
Role	Responsibilities
Management (first and second lines)	• Design and perform continuous monitoring to assess the adequacy and effectiveness of risk management and control. • Apply process expertise and act on risk. • Develop and implement management resolutions that address root causes. • Increase timeliness of corrective actions.

Internal audit function (third line)	• Plan continuous auditing jointly with the first and second lines.
	• Perform continuous auditing:
	  ○ Relate analytics to assertions and business objectives.
	  ○ Align risk factors and control activities.
	  ○ Add value by assessing emerging enterprise risks and opportunities.
	• Perform audit testing of continuous monitoring.
	• Provide continuous assurance in connection with audit objectives such as completeness and accuracy.
	• Maintain effective data security arrangements.

Foundational Continuous Assurance Framework

A foundational continuous assurance framework encompasses the internal audit function's continuous auditing process and audit testing of continuous monitoring. As the third line providing assurance over management's enterprise risk management and control processes, internal auditors strive to identify areas of concern within the control framework to provide the organization with the highest feasible level of independent and objective assurance.

Figure 3. Foundational Continuous Assurance Framework



Continuous Auditing

Continuous auditing is achieved through ongoing risk and control assessments enabled by technology-based audit techniques. These techniques have traditionally been related to generalized audit software, spreadsheet software or scripts developed using audit-specific software, specialized audit utilities, commercially packaged solutions, and custom-developed production systems. Innovative technologies that enable and enhance continuous auditing include:

- Artificial intelligence (AI).
- Natural language processing (NLP).
- Robotic process automation (RPA).

Audit techniques should be flexible and scalable to play a key role in optimizing the:

- Timely identification of anomalies (potential findings).
- Analysis of patterns and trends.
- Detailed transaction analysis against cut-off thresholds.
- Analysis of entire populations.
- Automation of data collection.
- Testing of controls.
- Comparative analysis among peers or benchmarking.

Continuous auditing analyzes systems for changes, security, incidents, anomalies, and transactions, enabling the identification of risk indicators and evaluation of risk parameters across IT operations, IT applications, and business processes. Continuous auditing enhances the internal audit function's ability to advise and provide assurance on the availability and utility of data, understand application controls, and optimize business processes through automation (Standard 14.4 Recommendations and Action Plans). When deployed effectively, continuous auditing:

- Focuses on **engagement objectives** and assertions such as completeness, accuracy, and authorization to determine the reliability of the information decision-makers use.
- Can detect emerging risk areas where controls are weak and recommend them for corrective action.

The foundational continuous assurance framework shown in Figure 3 illustrates that overlap between continuous auditing and continuous monitoring can be avoided, and continuous auditing can be performed even if continuous monitoring is absent in the first and second lines. However, opportunities for continuous monitoring exist wherever there are opportunities for continuous auditing. Continuous auditing presents valuable opportunities for **findings** and recommendations, enhancing oversight and risk management when fully utilized.

Technologies such as AI, NLP, RPA, and blockchain can significantly enhance continuous auditing programs by automating and streamlining various auditing tasks. For example, AI algorithms can analyze large amounts of data in real time, identifying anomalies, trends, and potential risks more efficiently than traditional or more manual methods. NLP can analyze and interpret unstructured data, such as emails, contracts, invoices, and reports to uncover insights and potential noncompliance that manual reviews might miss. RPA may enhance continuous auditing by automating repetitive and time-consuming tasks, such as data collection, analysis, and reporting. RPA **bots** can continuously review transactions and processes, flagging anomalies and potential risks in real time, allowing internal auditors to focus on more complex and strategic activities. Blockchain can be used to provide audit trails that cannot be altered. Together, these technologies enable continuous review and timely detection of irregularities that, if acted on, may help organizations maintain compliance and operational integrity.

Ongoing Assessments of Risks and Controls

Ongoing risk and control assessments should be structured to complement each other. AI-driven control assessments can continuously monitor and evaluate the effectiveness of controls, providing real-time feedback on control performance. NLP can analyze text data related to controls and assist in evaluating control effectiveness.

Ongoing Risk Assessment

Ongoing risk assessment is the continual identification and assessment of risks to the achievement of business objectives using technology-based audit techniques. Ongoing risk assessment should include a review of the results of management's monitoring efforts, including leading indicators, performance measures, quality control, and the segregation of duties. Ongoing risk assessments use technology-based audit techniques to continually:

- Examine and analyze a single process to detect trends and anomalies compared with the process's own past performance and that of other processes or systems operating within the organization.
- Correlate and analyze anomalies showing management's risk responses and providing a forward-looking view on emerging risks.
- Employ technologies such as AI, NLP, and RPA to enhance data analysis, perform routine tasks, detect anomalies, provide predictive analytics, and automate complex tasks.
- Highlight potential risks to be included in engagements (periodic and real-time).
- Detect anomalies in business units, operating locations, or processes that may indicate increased risks or unexplained, atypical rates of change.
- Highlight areas over which controls are nonexistent or not performing inadequately, prompting auditors to perform more thorough control assessments in specific areas.
- Manage controls over business-critical spreadsheets and other user-developed applications.
- Predict or anticipate future risks.

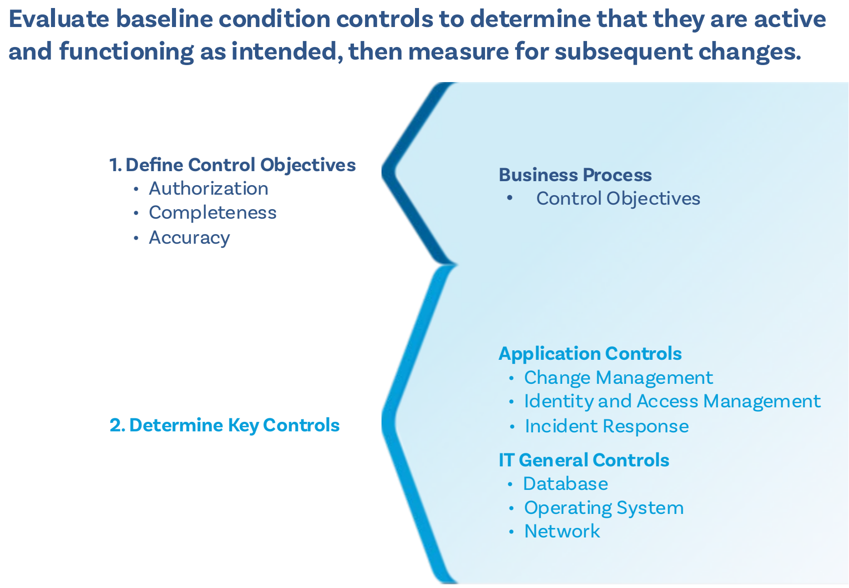
Ongoing risk assessment results serve as inputs for the internal audit plan and ongoing control assessment activities.

Ongoing Control Assessment

Ongoing control assessment continually evaluates controls against a baseline condition and uses technology-based audit techniques to evaluate subsequent changes to control configurations, considering the balance of automated controls, IT general controls, and manual controls as illustrated in Figure 4. In each case, internal auditors should look for unusual patterns or other anomalies. Ongoing control assessment:

- Enables chief audit executives to provide management with early warnings of control violations or deficiencies.
- Allows AI-driven control assessments to continuously monitor and evaluate the effectiveness of controls, providing real-time feedback.
- Uses NLP to analyze unstructured data related to control processes, identifying areas in which controls may be lacking or ineffective.

Figure 4. Ongoing Control Assessment



Ongoing control assessments can be effective without operating in real-time. The frequency of analysis should be determined by the level of risk, the business process cycle, the time required to set up and deploy the automated tools, and the degree to which management monitors the controls. For example:

- Purchase card analytics might be processed monthly after transaction statements are received from credit card companies.
- Payroll might be processed every pay period to synchronize with direct deposit transactions.
- Tests for duplicate invoices and payments could be run daily.
- Operating system patching might be scanned monthly.
- Changes to automated controls tend to be infrequent and might be monitored in coordination with IT's change release cycle.

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

Ongoing control assessment results, organized by process, should:

- Support audit engagement objectives.
- Communicate:
  - Conditions of key controls (security settings such as password length).
  - Changes to automated controls.

Continuous Monitoring

Management should own and perform continuous monitoring because this activity aligns with the responsibilities of the first and second lines. Many of the techniques management could use to continuously monitor controls are similar to the continuous auditing techniques used by internal auditors. Continuous monitoring principles include:

- *Planning* – Considering the business objective(s) and critical success factors.
- *Identifying Risk* – Determining the obstacles likely to inhibit the organization's success.
- *Configuring* – Aligning diverse sources of data, such as configurable conditions, changes, event logging, financial transactions, and unstructured data, to discover and corroborate emerging risks.
- *Timing* – Detecting control issues in real time.
- *Reporting* – Periodically (weekly, monthly) communicating the results of continuous monitoring efforts.
- *Monitoring* – Tracking identified deficiencies for remediation.

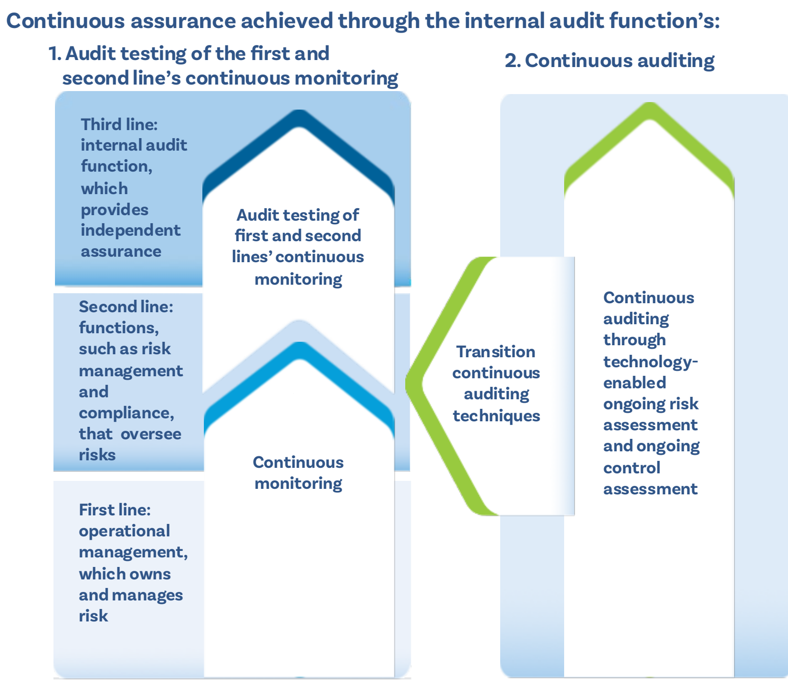
When implemented effectively, continuous monitoring can:

- Enhance the ability to promptly identify and curtail control problems.
- Reduce incidences of error and **fraud**.
- Enhance operational efficiency.
- Identify deviations from expected performance.
- 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

Internal auditors may be asked to provide **advisory services** to functions that own and manage risks and controls (first line) and the functions that oversee risks and controls (second line) by helping to design and implement policies, processes, or systems. Continuous assurance is optimized when technology-enabled continuous auditing techniques are used in the continuous monitoring efforts of the first and second lines, and those continuous monitoring efforts are reliable and responsive to risk.

Figure 5. Optimized Continuous Auditing Framework

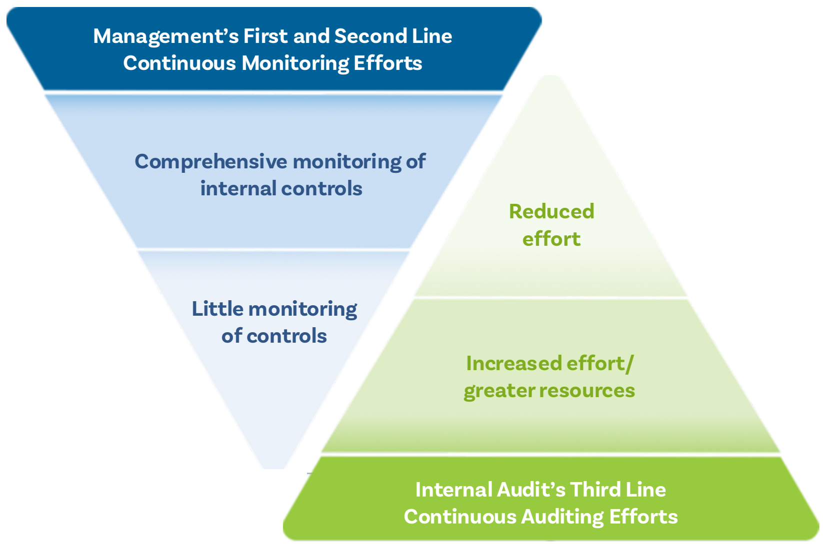


When management adopts continuous auditing techniques for continuous monitoring, careful coordination is essential to prevent overlap between the two processes and between the second and third lines (Standard 9.5 – Coordination and Reliance). When continuous auditing techniques are transitioned to management, care should be taken to ensure internal auditors do not assume ownership of continuous monitoring, which may impair their **independence** and **objectivity** (Principle 2 Maintain Objectivity).

Relationship Between Continuous Auditing and Continuous Monitoring

There is an inverse relationship between continuous auditing and continuous monitoring. All three lines contribute to measuring and strengthening the effectiveness of risk management and control. The internal audit function 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 is lacking or inconsistent, the internal audit function should increase its continuous auditing efforts accordingly, as illustrated in Figure 6.

Figure 6. Relationship Between Continuous Auditing and Continuous Monitoring Efforts



Where management has not implemented continuous monitoring, the internal audit function should enhance detailed testing through continuous auditing techniques. If the first or second line performs continuous monitoring on a comprehensive basis across end-to-end business process areas, internal auditors may scale back duplicative techniques within the continuous auditing program. In this case, it may be beneficial for internal auditors to determine whether the continuous monitoring process is reliable. Such procedures include reviews of:

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

Practical Applications for Continuous Auditing

Continuous auditing supports the work of internal auditors throughout an engagement. Continuous auditing can be applied to internal audit planning, audit engagement support, and monitoring the implementation of recommendations or action plans.

The chief audit executive should acknowledge that several second-line functions — such as enterprise risk management, compliance, ethics, and security — are closely connected to continuous auditing. The internal audit function should explore how continuous auditing can be used to evaluate these functions and consider relying on the insights they generate.

Internal Audit Plan Development

Continuous auditing enhances the development of the internal audit plan by enabling auditors to build a more risk-responsive audit universe. Rather than scheduling engagements according to a standard cycle of rotation, the frequency of engagements should be based on risk, complexity, pervasiveness, and the velocity of change. Continuous auditing helps internal auditors quickly identify changes in risks and potential exposure.

Application of Ongoing Risk Assessment

Data analytics should be used to develop leading indicators that trigger specific engagements or activities to be included in the audit plan. For example, when ongoing risk assessment is applied in a large-scope engagement, leading indicators may signal the locations to be visited or the focus of engagement objectives and scope or may even trigger an immediate walk-through of an activity where the risk has increased significantly without an adequate explanation (Standards 13.2 Engagement Risk Assessment and 13.3 Engagement Objectives and Scope).

AI can enhance the risk assessment process by providing predictive analytics that forecast potential risks based on historical data. NLP can analyze unstructured data to identify trends and emerging risks, allowing auditors to proactively address issues before they become significant problems.

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

- Applying a more strategic context to the development of audit plans and making ongoing plan adjustments when risk profiles change.
- Allocating the necessary audit resources to areas where risk exposure is unacceptable.
- Assessing management's risk mitigation activities.
- Developing areas of focus and strategic themes for the internal audit universe.

- Scoping and drafting objectives for individual engagements.

The key distinction between using ongoing risk assessment for enterprise audit planning versus for supporting an individual engagement is the level of detail needed. Summary-level information may be sufficient to find anomalies and redirect resources when developing the audit plan. Conversely, more detailed information would be necessary to identify risks and test controls to support the scope and objectives of audit engagements.

Figure 7. Continuous Auditing Throughout the Audit Process

Audit Engagement Support

Continuous auditing can be integral to audit fieldwork, and its techniques often improve and mature during an engagement. 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 comparison data alone is insufficient to attain the engagement objective.
- Identify risk indicators and assess critical controls.
- Detect symptoms of fraud, waste, and abuse through the identification of anomalies.
- Analyze large amounts of data in real time using AI to identify anomalies and control weaknesses.

- Use NLP to process unstructured data and provide insights previously unavailable to the average auditor.

Audit analytics and continuous auditing techniques differ in 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 from previous engagements, are conducted systematically and frequently during and beyond the scope and timeline of an engagement and provide timely notification of trends, patterns, and anomalies.

Application of Ongoing Risk Assessment

During an engagement, ongoing risk assessment can help the auditor better understand the business process. For example, examining payment types in accounts payable may reveal that one office uses electronic fund transfers while another produces manual checks. This information allows the auditor to better understand the process at each location and assess the risk accordingly.

Application of Ongoing Control Assessment

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

- Examining transactional data or data normally related to a business process or an economic event, such as an order, invoice, or payment (for example, flagging all purchase card transactions greater than the authorization limit or that involve prohibited merchants).
- Evaluating configurations:
    - Assessing systems to evaluate the status of configurable automated controls.
    - Reviewing approval levels and access capabilities.
- Assessing program and parameter changes.
- Scanning incident and error management.
- Reviewing summarized data (for example, if a cardholder's total monthly transactions are greater than US$10,000 but the cardholder is outside the purchasing function).
- Employing comparative analysis (for example, total overtime payments compared to all other employees in the same job classification or overtime compared to thresholds).
- Testing general ledger account balances (for example, highlighting accounts in which 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.
- Using AI models to analyze financial transactions in real time to detect irregularities such as duplicate payments, unauthorized access, or policy violations.
- Using NLP to extract key clauses, identify missing terms, and flag noncompliance in contracts or policy documents. Additionally, NLP can be used to monitor internal communications for signs of collusion, policy violations, or unethical behavior.
- Using RPA bots to pull data from ERP systems, spreadsheets, or databases on a scheduled basis to feed into audit analytics tools. Also, RPA can be utilized to automate the reconciliation of accounts, transactions, or inventory by comparing data across systems and flagging discrepancies.

Ongoing control assessments enable auditors to quickly scrutinize details, evaluate potential causes, and recommend appropriate remediation plans promptly.

Confirming the Implementation of Recommendations or Action Plans

Ongoing risk assessment can be used to follow up on engagement findings promptly, making it a powerful tool in ensuring continuous improvement and heightened performance (Standard 15.2 Confirming the Implementation of Recommendations or Action Plans). Following an engagement, auditors can use ongoing risk assessment to verify the implementation of recommendations and assess the effectiveness of management's action plans.

Management's action plans should identify performance indicators to evaluate successful remediation. Performance indicators simplify establishing a baseline and enable comparisons of results before and after recommendations or action plans have been implemented. Internal auditors should collaborate with management to identify relevant indicators that can be measured systematically.

Continuous Auditing Implementation

Successfully implementing continuous auditing requires leadership, change management, and a phased approach that initially addresses the most critical business systems. Although each organization is unique, the common steps shown in Figure 8 should be carefully planned and managed when developing and implementing continuous auditing.

Figure 8. Key Steps to Implementing Continuous Auditing

Internal auditors can tailor the sequence of steps in the figure to an organization's needs and may add activities to support continuous auditing.

Establish a Continuous Auditing Strategy

Standard 9.2 states, "The chief audit executive must develop and implement a strategy for the internal audit function that supports the strategic objectives and success of the organization and aligns with the expectations of the board, senior management, and other key stakeholders." The internal audit strategy could include a short-term initiative introducing continuous auditing to support engagements to assess regulatory compliance. However, enhanced business performance can be a significant additional benefit of adopting continuous auditing.

Coordinate with the First and Second Lines

Senior management should encourage business and IT acceptance of the continuous auditing strategy. The internal audit function should assess the end-to-end business process and interdependent IT controls. The reliability of business systems and transactional data is essential for maintaining a strong control framework, ensuring financial reporting integrity and optimizing business operations efficiency. Ensuring the reliability, integrity, and availability of business systems and data should be a key objective for the chief audit executive and senior management. Continuous auditing can support this objective by facilitating assessments of risk management and control processes.

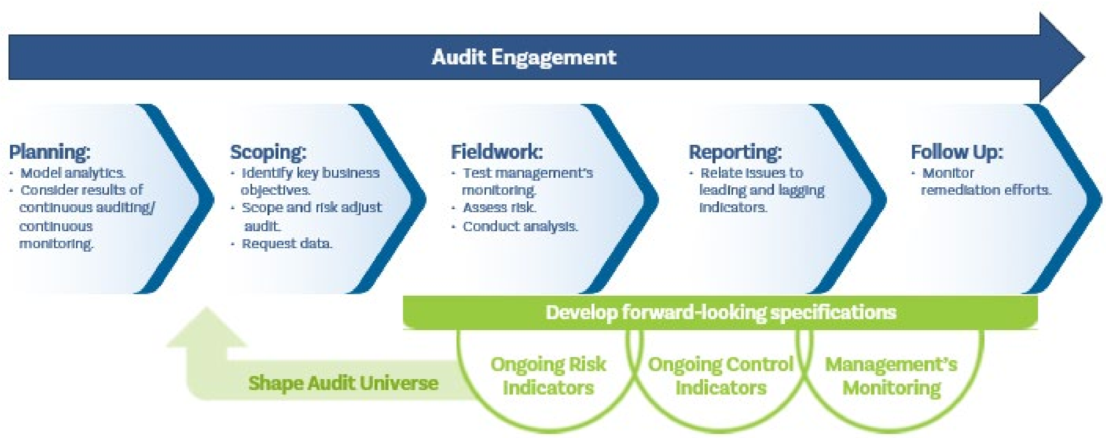
Set Priorities and Gain Management Support

Continuous auditing requires continual access to production applications and data. Reliable technologies may require significant investment and multiyear implementation efforts. Support from the board and senior management is essential. A strategy that includes phased implementation over two or more years may help manage the pace and expectations and steadily demonstrate the benefits of continuous auditing technologies and **methodologies**.

Adapt the Audit Plan to Specify Ongoing Indicators

The strategy should include major processes or activities, such as procurement-to-pay or customer-to-cash. Continuous auditing techniques should be applied to three related risk categories: IT operations, applications, and business process transactions. Audit analytics can be used to design specifications for risk and control indicators. The chief audit executive can align the internal audit plan to identify process areas and engagements, defining key risk indicators and control metrics for ongoing assessment. Scheduled engagements allow management and the internal audit function to jointly assess leading and lagging indicators, measuring risk and controls in relation to business objectives. **Engagement results** can then be used to develop forward-looking specifications, as shown in Figure 9.

Figure 9. Develop Forward-Looking Specifications for Risk and Control Indicators



Acquire Data for Routine Use

Continuous auditing is more than just a technical endeavor, but selecting available technologies is essential to long-term success. The continuous auditing strategy should guide the selection of software solutions. When selecting continuous auditing technologies, the chief audit executive should consider options and capabilities already in organizational use. It is important to connect the program with the organization's computing environment and plans for key business systems.

Audit-specific analytic software solutions provide flexibility and can read diverse data types, including data from enterprise resource applications, such as SAP, Oracle, and other core business systems, as well as mainframe legacy, client/server, and internet-enabled systems.

Note

The IIA's GTAG "Understanding and Auditing Big Data" provides more information on core business systems and applications.

Establish Routine Access to the Production Environment

The chief audit executive should work with management to affirm that audit technology is compatible with the enterprise IT environment and that the internal audit function's access and use of business system data has a neutral **impact** on the operational performance of the production environment and related systems. The internal audit function should assess applicable privacy regulations and uphold privacy and security standards that meet or exceed those maintained in the production environment.

Develop Analysis Capabilities

Analysis capabilities should align with the continuous auditing strategy and business objectives before automating monitoring. Continuous auditing evidence is often 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 assist auditors in choosing the transfer method, schedule, and data protocol best suited for continuous auditing. Additionally, AI, NLP, and RPA tools can provide real-time analysis of structured and unstructured data.

Build Auditors' Technical Skills and Knowledge

Standards 3.1 Competency, 3.2 Continuing Professional Development, and 4.2 Due Professional Care require that the internal audit function collectively possess or obtain the **competencies** needed to perform its responsibilities. Varying levels of IT and AI proficiency will be required as continuous auditing is developed and implemented. Note that emerging AI, NLP, and RPA tools tend to have more user-friendly and intuitive interfaces that facilitate using the technology without an extensive technical background. Some items to consider in the early stages of implementation are:

- 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, internal auditors should:

- Review key data fields and data elements.
- Review metadata created by functions applied to the data.

- Ascertain the timeliness of the data.
- Establish how frequently the information is updated.
- Determine who can modify, change, or delete data.
- Verify when the last update occurred.
- Determine whether the information is complete and accurate.
- Verify assumptions and analysis with application programmers.
- Verify data integrity by performing various tests such as reasonability, edit checks, and comparison to other sources, including previous investigations or audit reports.
- Apply knowledge gained from internal audit engagements.

Assess Reliability of Data Sources

Data reliability is critical to successfully implementing continuous auditing and should be assessed during a baseline audit. Data from a production environment governed by IT general controls is more reliable than data from end-user developed applications. As reliability increases, the level of testing and verification necessary to reduce audit risk to an acceptable level decreases.

Note

The IIA's GTAG "Auditing Business Applications" provides more information on user-developed applications.

Prepare and Validate Data

Robust validation capabilities and **criteria** are essential to ensure the data's integrity before it is analyzed (Standard 13.4 Evaluation Criteria). A key strength of continuous auditing is its ability to extract and integrate data from diverse systems across the organization for comprehensive analysis. Combining data from multiple systems requires validation to identify and 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. Additionally, newer technologies such as blockchain can provide unalterable data tracking to help with validation.

Construct Continuous Auditing Indicators

Internal auditors should create a structured plan that integrates seamlessly with the auditing process. The plan should include continuous auditing techniques that are designed and constructed based on insights and specifications resulting from previously conducted engagements.

Ongoing Risk Assessment

Consistent with Standard 9.1 Understanding Governance, Risk Management, and Control Processes, continuous auditing enables auditors to "oversee risk management and control" and "communicate risk and control information" in a timely manner.

Key activities and considerations in performing ongoing risk assessment include:

- Developing 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 sensitive to change.
    - Use risk assessment results to potentially modify audit plans, as well as individual audit scopes and objectives. AI enhances risk assessment by providing predictive analytics that can forecast potential risks based on historical data.
- Designing analytics to measure increased levels of risk. Key risk indicators should:
    - Focus on the extent of change experienced by the activity under review over time (be designed to enable trend analysis).
    - Comprise a combination of process-based leading indicators and symptomatic lagging indicators.
    - Enable routine comparisons, highlighting anomalous entries that exceed established **risk tolerance** levels.

Ongoing Control Assessment

Ongoing control assessment provides independent analyses 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 prior to symptomatic errors in data, ongoing control assessment enables management to receive early warnings about control performance.

The true power of ongoing control assessment lies in the ability to provide relevant assurance effectively and promptly. Key activities and considerations in performing ongoing control assessment include:

- Thoughtful design of control objectives.
    - Internal auditors should identify a smaller number of analytics that relate to high-level control objectives, rather than automating each step of an existing engagement work program.
    - 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. Joint discussions with management and technology experts may provide an understanding of automated controls.

- Determining key controls.
    - Walking through a business scenario to consider what could go wrong to determine how the system's automated techniques have been designed and configured to mitigate identified risks by controlling the authorization, completeness, and accuracy of transactions.
    - Interrogating configured controls systematically to determine their current and baseline conditions enables evaluating whether they are operating effectively as designed.
    - Monitoring changes to automated, configurable controls enables determining the level of confidence in the their effectiveness. Automated controls that are not configured well or that change frequently decrease confidence.
- Evaluating the baseline condition of controls.
    - Once key business processes, related control objectives, and automated controls are defined, ranking them allows critical control points (highest impact/risk) to be identified.
    - For critical control points, appropriate analytics for each control objective should be defined.
    - The current condition of configured automated controls should be compared to a baseline value.
    - The assessment should determine whether the condition of the configured automated controls has changed since the prior baseline engagement, and if it has, determine whether the change was authorized and appropriate.
    - The assessment should ensure transaction anomalies are reviewed to validate the controls' effectiveness.

Report and Manage Results

Once continuous auditing indicators are designed and implemented, the internal audit function should plan ongoing assessments of risks and controls aligned with the internal audit plan. Ongoing assessments should include analyzing the results of the continuous auditing techniques, exploring as necessary, and developing recommendations and/or collaborating with management to develop action plans.

Deliverables can range from straightforward graphics of comparisons and trends to data visualization of risks and controls (see Appendix C). The process is iterative, with proficiency in continuous auditing and monitoring strengthening as internal auditors collaborate with the first and second lines (Standards 3.1 Competency and 9.5 Coordination and Reliance). Implementing effective continuous auditing and continuous monitoring programs promotes timely decision-making, coordinated action plans, and successful remediation of findings (Standards 14.4

Recommendations and Action Plans and 15.2 Confirming the Implementation of Recommendations or Action Plans).

Establish a Repeatable Methodology

A structured methodology for managing results should include steps to ensure that findings identified are addressed and remediated promptly.

For example:

- Reviewing and analyzing potential findings to measure risk with increasing accuracy.
- Performing **root cause** analysis to identify weaknesses in control design, execution, or both.
- Addressing root causes to deter recurring findings, which can lead to better recommendations and highlight the advantages of a continuous auditing methodology.
- Recording and tracking management's action plans for resolving findings.

Report Results

Reporting strategies range from simply exporting findings into a shared folder on a network drive to email notifications, system to track the remediation of findings, dashboards, and data visualization (Standard 11.3 Communicating Results). Various reporting solutions may be implemented to meet the needs of the first, second, and third lines, senior management, and the board.

Key considerations for reporting continuous auditing results include:

- Publishing comprehensive reports at the level of detail required to support continuous auditing and continuous monitoring.
- Storing results in a secure database.
- Presenting trending information in a web-based dashboard or heat map.

The method used to communicate results should reflect the intended audience. More detailed and timely results are useful for operational teams, while dashboards and heat maps may benefit the board or senior management.

Facilitate Management Action

Each action plan should identify an owner, the individual responsible for addressing the findings, and the planned date of completion. When actions have been completed, action plans should be reported as resolved, and subsequent continuous monitoring should measure whether the action plans have effectively addressed the findings (Standard 15.2 Confirming the Implementation of Recommendations or Action Plans).

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 chief audit executive should **periodically** refresh the continuous auditing program strategy to adapt to new priorities and themes. Over time, thresholds, control tests, and parameters for various analytics may need to be strengthened or relaxed. Additional control points or risk exposures may need to be added, and others may be transitioned to management's continuous monitoring efforts.

The chief audit executive should record the benefits realized by implementing continuous monitoring in other management initiatives, such as enterprise risk management and measurement of control performance. Quantifying the benefits gained by internal auditors and other assurance providers documents return on investment, enhances reputation, and justifies funding for further investment and strategic development.

Appendix A. Relevant IIA Standards and Guidance

The following IIA resources were referenced in this guide.

Standards and Principles
Principle 2 Maintain Objectivity
Standard 3.1 Competency
Standard 3.2 Continuing Professional Development
Standard 4.2 Due Professional Care
Standard 6.3 Board and Senior Management Support
Standard 9.1 Understanding Governance, Risk Management, and Control Processes
Standard 9.4 Internal Audit Plan
Standard 9.5 Coordination and Reliance
Standard 10.1 Financial Resources
Standard 10.2 Human Resources Management
Standard 10.3 Technological Resources
Standard 11.3 Communicating Results
Standard 12.2 Performance Measurement
Standard 13.3 Engagement Objectives and Scope
Standard 13.4 Evaluation Criteria
Standard 13.5 Engagement Resources
Standard 14.4 Recommendations and Action Plans
Standard 15.1 Final Engagement Communication
Standard 15.2 Confirming the Implementation of Recommendations or Action Plans
Global Guidance and Other IIA Resources
Global Practice Guide "Coordination and Reliance: Working with Other Assurance Providers"
Global Technology Audit Guide "Auditing Business Applications"
Global Technology Audit Guide "Understanding and Auditing Big Data"
The IIA's *Three Lines Model: An Update of the Three Lines of Defense*

Appendix B. Glossary

Definitions are taken from the "Glossary" within The IIA's publication, Global Internal Audit Standards, 2024 Edition, unless otherwise noted as being from these or other footnoted sources:

- IBM, https://www.ibm.com/think/topics, accessed September 25, 2025.
- ISACA, "Glossary," Information technology terms and definitions, accessed September 25, 2025. https://www.isaca.org/resources/glossary.
- Merriam-Webster.com Dictionary, Merriam-Webster, accessed September 25, 2025. https://www.merriam-webster.com/.
- NIST Computer Security Resource Center, "Glossary," accessed September 25, 2025. https://csrc.nist.gov/glossary.

advisory services – Services through which internal auditors provide advice to an organization's stakeholders without providing assurance or taking on management responsibilities. The nature and scope of advisory services are subject to agreement with relevant stakeholders. Examples include advising on the design and implementation of new policies, processes, systems, and products; providing forensic services; providing training; and facilitating discussions about risks and controls. "Advisory services" are also known as "consulting services."

application – A computer program or set of programs that performs the processing of records for a specific function. *Scope Notes*: Applications contrast with systems programs, such as an operating system or network control program, and with utility programs, such as copy or sort [ISACA Glossary].

artificial intelligence – A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments [NIST Glossary].

assurance – Statement intended to increase the level of stakeholders' confidence about an organization's governance, risk management, and control processes over an issue, condition, subject matter, or activity under review when compared to established criteria.

blockchain – A distributed digital ledger of cryptographically-signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules [NIST Glossary].

board – Highest-level body charged with governance, such as:

- A board of directors.
- An audit committee.
- A board of governors or trustees.
- A group of elected officials or political appointees.
- Another body that has authority over the relevant governance functions.

In an organization that has more than one governing body, "board" refers to the body or bodies authorized to provide the internal audit function with the appropriate authority, role, and responsibilities.

If none of the above exists, "board" should be read as referring to the group or person that acts as the organization's highest-level governing body. Examples include the head of the organization and senior management.

bot – a computer program that performs automatic repetitive tasks. [Merriam-Webster.com Dictionary]

chief audit executive – The leadership role responsible for effectively managing all aspects of the internal audit function and ensuring the quality performance of internal audit services in accordance with Global Internal Audit Standards. The specific job title and/or responsibilities may vary across organizations.

compliance – Adherence to laws, regulations, contracts, policies, procedures, and other requirements.

configuration – The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged [NIST Glossary].

control(s) – Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.

control process – The policies, procedures, and activities designed and operated to manage risks to be within the level of an organization's risk tolerance.

criteria – In an engagement, specifications of the desired state of the activity under review (also called "evaluation criteria").

engagement – A specific internal audit assignment or project that includes multiple tasks or activities designed to accomplish a specific set of related objectives. See also "assurance services" and "advisory services."

engagement objectives – Statements that articulate the purpose of an engagement and describe the specific goals to be achieved.

engagement results – The findings and conclusion of an engagement. Engagement results may also include recommendations and/or action plans.

finding – In an engagement, the determination that a gap exists between the evaluation criteria and the condition of the activity under review. Other terms, such as "observations," may be used.

fraud – Any intentional act characterized by deceit, concealment, dishonesty, misappropriation of assets or information, forgery, or violation of trust perpetrated by individuals or organizations to secure unjust or illegal personal or business advantage.

governance – The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

impact – The result or effect of an event. The event may have a positive or negative effect on the organization's strategy or business objectives.

incident – A violation or imminent threat of violation of computer security policies, acceptable use policies, guidelines, or standard security practices [ISACA Glossary].

independence – The freedom from conditions that may impair the ability of the internal audit function to carry out internal audit responsibilities in an unbiased manner.

integrity – Behavior characterized by adherence to moral and ethical principles, including demonstrating honesty and the professional courage to act based on relevant facts.

internal audit function – A professional individual or group responsible for providing an organization with assurance and advisory services.

internal audit plan – A document, developed by the chief audit executive, that identifies the engagements and other internal audit services anticipated to be provided during a given period. The plan should be risk-based and dynamic, reflecting timely adjustments in response to changes affecting the organization.

internal auditing – An independent, objective assurance and advisory service designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.

methodologies – Policies, processes, and procedures established by the chief audit executive to guide the internal audit function and enhance its effectiveness.

natural language programming/processing - Enables computers to analyze and manipulate human language using various techniques, such as text analysis, sentiment analysis, machine translation, and speech recognition, to complete tasks like summarizing information, generating human-like text, and translating language [ISACA Glossary].

objectivity – An unbiased mental attitude that allows internal auditors to make professional judgments, fulfill their responsibilities, and achieve the Purpose of Internal Auditing without compromise.

periodically - At regularly occurring intervals, depending on the needs of the organization, including the internal audit function.

results of internal audit services – Outcomes, such as engagement conclusions, themes (such as effective practices or root causes), and conclusions at the level of the business unit or organization.

risk – The positive or negative effect of uncertainty on objectives.

risk assessment – The identification and analysis of risks relevant to the achievement of an organization's objectives. The significance of risks is typically assessed in terms of impact and likelihood.

risk management – A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

risk tolerance – Acceptable variations in performance related to achieving objectives.

robotic process automation – Uses intelligent automation technologies to perform repetitive office tasks of human workers, such as extracting data, filling in forms, moving files and more [IBM).

root cause – Core issue or underlying reason for the difference between the criteria and the condition of an activity under review.

senior management – The highest level of executive management of an organization that is ultimately accountable to the board for executing the organization's strategic decisions, typically a group of persons that includes the chief executive officer or head of the organization.

significance – The relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors, such as magnitude, nature, relevance, and impact. Professional judgment assists internal auditors when evaluating the significance of matters within the context of the relevant objectives.

stakeholder – A party with a direct or indirect interest in an organization's activities and outcomes. Stakeholders may include the board, management, employees, customers, vendors, shareholders, regulatory agencies, financial institutions, external auditors, the public, and others.

Appendix C. Ongoing Risk Assessment Case Study

This case study outlines a program for internal auditors to develop and implement ongoing risk assessment for the manual journal voucher process.

Ongoing process-level risk assessment can:

- Identify new and emerging risks that occur shortly after the associated initial transaction.
- Help auditors identify abnormal trends, assess cumulative impact, and calculate the total value at risk.

Understand the Process

The first step in developing ongoing risk assessment is to understand the activity or process being assessed. In this case, internal auditors conducted external research and gathered relevant information from management and process owners to understand the total population, available reports, nonstandard areas, and dependencies on other processes. This information helped internal auditors build a prototype database of risk attributes that could impact the manual journal voucher process.

Create a Prototype Risk Database

Internal auditors used analytical and statistical tools to iteratively develop a prototype risk database, ensuring data integrity, completeness, and logic accuracy.

For example, the risk attributes of the manual journal voucher (MJV) database included:

Risk Outcomes

MJV impacts on:

- Net profit.
- Revenue and expenses.
- Cash and other assets.

Risk Indicators

MJVs posted:

- By terminated users or unauthorized users.
- After the cut-off date.

- On holidays.
- Without adequate segregation of duties.
- Without documentation or approvals.
- Transactions in excess of approved value thresholds.
- Entries appear to be split transactions to evade approved value thresholds.

Identify Unknown Risks and Anomalies Using Statistical Techniques

Internal auditors applied statistical techniques, including grid, cluster, Benford's Law, and regression analyses, to identify new and emerging risks.

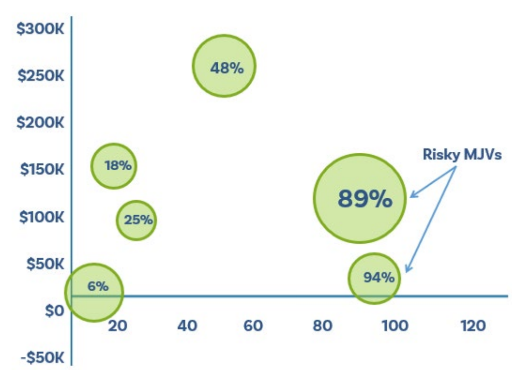
Grid analysis segmented the population by two independent variables: manual journal voucher percentage (MJV%) and trial balance dollars (TB$). Figure 10 depicts 10 countries in a grid to help visualize risk. The countries that performed well were asked to share best practices.

Figure 10. Grid analysis of countries MJV percentage and trial balance amount

		TB Amount $		
		< 1 Million	1 to 4 Million	> 4 Million
MJV Amount (%)		1	2	4
0% to 9%	1	Country A	Country I	Country H
10% to 29%	2	Country B Country C	Country G	Country E Country F
> 30%	3		Country J	Country D

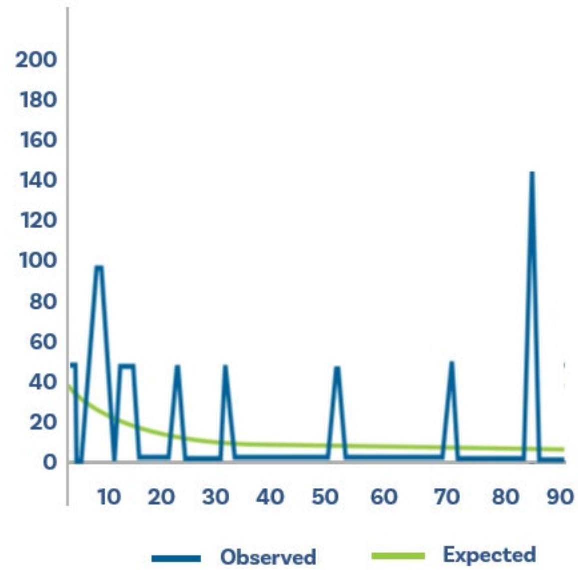
The cluster analysis shown in Figure 11 segments the population and identifies clusters of risky transactions across variables, such as high-dollar value, holiday postings, and year-end transactions.

Figure 11. Cluster analysis



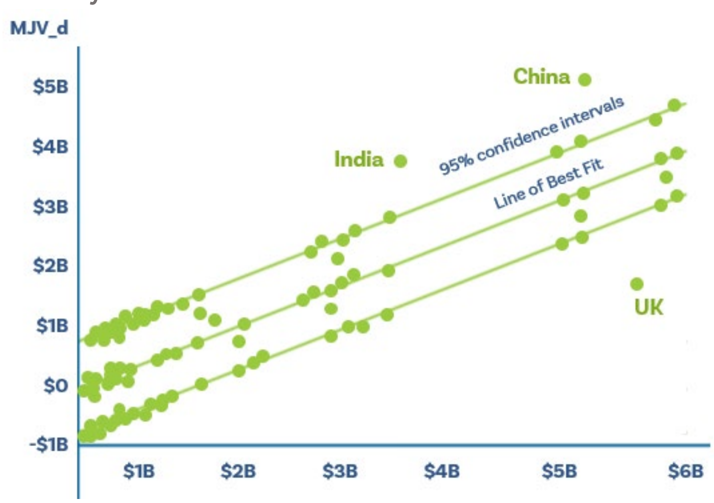
Benford's Law was used to analyze the occurrence of certain digits within key numeric fields to find abnormal, fabricated, or potentially fraudulent patterns. Figure 12 illustrates an abnormal trend analysis for one country.

Figure 12. Numeric trend analysis



Regression analysis was used to identify outliers, as shown in Figure 13. In this example, regression analysis identified nonconforming countries by plotting the total value of the MJV against the trial balance.

Figure 13. Regression analysis



Collaborate on Reporting Findings

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 the process was expanded to include management dashboards. The coordinated risk assessment dashboards prevented the duplication of data and efforts 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. The internal audit function maintained its independence by leaving the ownership of risks to others. Continuous monitoring reports informed management's action plans and provided enhanced opportunities to deter fraud and avoid unexpected risk events.

Appendix D. References and Additional Reading

IBM. “Explainers. Featured Topics.” *IBM Think.* Accessed September 25, 2025. https://www.ibm.com/think/topics.

ISACA. *COBIT, an ISACA Framework.* Accessed September 25, 2025. https://www.isaca.org/resources/cobit.

ISACA. “Glossary.” *Information Technology Terms and Definitions.* Accessed September 25, 2025. https://www.isaca.org/resources/glossary.

Joint Task Force. *NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations, Revision 5.2.0.* Gaithersburg, MD: NIST, August 2025. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_2_0/home.

NIST Computer Security Resource Center. “Glossary.” Accessed September 25, 2025. https://csrc.nist.gov/glossary.

About The Institute of Internal Auditors

The IIA is an international professional association that serves more than 265,000 global members and has awarded more than 200,000 Certified Internal Auditor® (CIA®) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

Disclaimer

Volunteer

To learn more about contributing to Global Guidance, visit https://www.theiia.org/end/about-us/get-involved/volunteer-your-time/.

Copyright

September 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101