KPMG

cutting through complexity

Leveraging data analytics and continuous auditing processes for improved audit planning, effectiveness, and efficiency

kpmg.com

Executive summary

Data analytics and continuous auditing are not new concepts, but their appeal appears to be rising. According to interviews with KPMG clients, the desire to effectively leverage data analytics and achieve continuous auditing within an internal audit function remains strong. And amid today's complex business environment, it is easy to see why.

Organizations are increasingly exposed to a variety of new risks such as growing compliance regulations, fraud schemes, operational inefficiencies, and errors that can lead to financial loss or reputational damage. As a result, organizational efforts to adopt innovative ways to assess and manage risk and enhance performance are critical. And that's where data analytics and continuous auditing are helping. If implemented properly, data analytics and continuous auditing have long been viewed as processes that can help Internal Audit departments simplify and improve the audit process through increasing operational efficiencies, reducing costs, and detecting potential fraud, errors, and abuse earlier—all while providing a higher quality audit. It is also increasingly becoming a way for organizations to create value.

The use of data analytics tools and techniques is helping to fundamentally transform and improve audit approaches. Consider the traditional audit approach, which is based on a cyclical process that involves manually identifying control objectives, assessing and testing controls, performing tests, and sampling only a small population to measure control effectiveness or operational performance. Fast forward to a continuous auditing approach using repeatable and sustainable data analytics and the approach becomes much more risk-based and comprehensive. With data analytics, organizations have the ability to review every transaction—not just a sampling—which enables a more efficient analysis on a greater scale. In addition, leveraging data analytics also accommodates the growing risk-based focus on fraud detection and regulatory compliance.

So, what are the most common scenarios seen today for implementing continuous auditing? How can your organization take a similar approach? What steps are needed to secure successful implementation? How are Internal Audit departments best leveraging data analytics? This paper explores common scenarios and applications that describe how leading organizations and Internal Audit departments are using continuous auditing techniques and leveraging data analytics to achieve audit objectives. It also identifies some of the common pitfalls that can be avoided through awareness and proper planning. In addition, it provides insight on how to move forward with your data analytics and continuous auditing plans.

Realizing the role and benefits of continuous auditing

The current economic climate encourages cost-cutting activities, increased risk exposure, and organizational changes. As a result, companies are employing continuous auditing (CA) techniques to manage risk as well as reduce cost, improve performance, and create value. Additional drivers include an ever-changing regulatory landscape—particularly in the financial services, healthcare, and public sectors—and increasing stakeholder demands to improve governance capabilities, enhance oversight and transparency, and manage risk while driving performance and profitability.

But what exactly is CA? While definitions may vary (see definitions below), CA is often confused with continuous monitoring (CM) since they share similar characteristics. For instance, both incorporate a wide variety of organizational data, integrate technology-enabled processes, and include analytic capabilities. Yet, CA and CM are distinctly different functions. The most obvious difference is that CA is a function of internal audit, while CM is the responsibility of management. This leads to an even greater differentiator: the roles that CA and CM play in enterprise-wide risk management. Essentially, CM, driven by management, can serve as the first two lines of defense—the business owners and the standard setters—within an organization's risk management framework. For example, CM processes can become key elements of an internal control environment. In contrast, CA, as an internal audit function, can serve as providing the primary assurance within the third line of defense for a company.

Continuous auditing (CA) is the collection of audit evidence and indicators by an internal auditor on information technology (IT) systems, processes, transactions, and controls on a frequent repeatable, and sustainable basis. It incorporates the manual continuous risk assessment process, which is largely qualitative analysis combined with quantitative technology-based data analytic processes.

Continuous monitoring (CM) is a feedback mechanism used by management to ensure that controls operate as designed and transactions are processed as prescribed. This monitoring method is the responsibility of management and can form an important element of the internal control environment.

Data analytics is an analytical process by which insights are extracted from operational, financial, and other forms of electronic data internal or external to the organization. These insights can be historical, real-time, or predictive and can also be risk-focused (e.g., controls effectiveness, fraud, waste, abuse, policy/regulatory noncompliance) or performance-focused (e.g., increased sales, decreased costs, improved profitability, etc.) and frequently provide the "how?" and "why?" answers to the initial "what?" questions frequently found in the information initially extracted from the data.

Organizations that work to draw maximum value from CA and CM tend to use a combination of both throughout the business. While neither CA nor CM needs to be present for the other to be implemented, companies that combine them tend to coordinate the efforts of internal audit with management to avoid duplication of efforts and unproductive use of resources.

Some organizations that have successfully implemented CA without having a CM process in place did so to better understand risks to the enterprise, assess control effectiveness, support compliance efforts, and better manage and utilize their internal audit resources. Often, CA techniques lead management to ultimately adopt select procedures as CM.

Three lines of defense

As an internal audit function, CA can serve as part of the third line of defense in a company's risk management framework.

Continuous monitoring (CM)		Continuous auditing (CA)
Business owners – *First line of defense*	**Standard setters –** *Second line of defense*	**Assurance providers –** *Third line of defense*
Business owners have risk content ownership. They are responsible for identifying and managing risks incurred over the course of daily business. Such risks may be operational in nature or may have to do with finance and compliance. The risks may represent discrete events rather than ongoing exposure. In addition to complying with risk management policies, business owners are expected to identify and assess emerging exposure.	Standard setters own risk processes and specific monitoring responsibilities. They establish policies and procedures handling risk; provide guidance and coordination among all stakeholders; identify enterprise trends, synergies, and opportunities for a change; and operationalize new events. In addition to facilitating critical liaison between business owners and assurance providers, standard setters provide oversight within specific risk areas (such as credit), and in terms of specific enterprise objectives (such as compliance).	Assurance providers ensure that the company is achieving business objectives, mitigating and managing risks, and optimizing risk management process effectiveness. Internal Audit often serves as the primary assurance provider in the third line of defense for many companies. Assurance providers are responsible for setting standards for risk management, ensuring that these are well understood, broadly embraced, and adequate for the company's needs. Assurance providers liaise with senior management or the corporate board to enable visibility into enterprise risk management activities.

A foundation in data analytics

Most internal audit organizations recognize the value and benefits of CA. However, they may lack the resources, both financial and human, or capabilities to design and implement CA processes initially. As a result, many of these organizations are beginning to lay the foundation by effectively utilizing data analytics to begin on their path toward more mature repeatable and sustainable CA processes.

In leveraging data analytics, Internal Audit departments have traditionally focused on transactional-based analytics to identify exceptions in populations when applying selected business rules-based filters in key areas of risk such as revenue or procurement. These transactional, rules-based analytics, or "micro-level" analytics, can provide significant value for known conditions where assessment of the frequency and magnitude of the condition needs to be performed. Leading internal audit organizations are realizing value by leveraging business intelligence-based tools and techniques to perform "macro-level" analytics to identify broader patterns and trends of risk and, if necessary, apply more traditional "micro-level" analytics to evaluate the magnitude and scope of items or issues identified through the "macro-level" analytics.

Internal audit… then and now

Changing times call for changing measures. This is evident in the comparison on the right, which highlights the changing role of internal audit within an organization:

Historical:

- Cyclical-based auditing
- Focus on coverage of audit universe
- Sampling small percentage of population
- End-to-end audits of processes/ business units
- Limited data mining on audits

Current:

- Shift from value preservation to value creation – evolving skills set
- "Pressure to be lean" – more focused audits based on emerging risk indicators; use of dynamic audit planning
- Regulatory compliance and/or fraud detection emphasis
- Control and transaction-testing based on underlying risk
- Risk-based data gathering and more efficient analysis of a larger population

Common applications of data analytics in an internal audit environment

Less mature state		More mature state	
Macro-level analytics for risk - or performance-focused process assessments • Broadly focused, not a very deep dive • Used for high-level audits or for high-level risk assessments for audit determination	Macro- and micro-level analytics for special audit projects • Narrowly focused on an area or issue and can include a deep dive	Macro- and sustained micro-level analytics for quantitative-based risk assessment for audit planning purposes • Repeatable and sustainable, continuous risk assessment process for dynamic audit planning purposes and moving toward CA enablement	Macro- and sustained micro-level analytics for controls testing and/or compliance auditing • Optimized in a repeatable and sustainable process maturing to a CA/CM process

Essentially, a mature data analytics process benefits the internal audit function by automating the collection, formatting, and mapping of key organizational data, and applying various tools to analyze and interpret the data in a more meaningful and effective way. This results in more focused audits that have the ability to zero in on specific areas of risk, conduct more dynamic audit planning, and seek a greater balance of controls versus transaction analysis based on underlying risk. If deployed appropriately, the use of data analytics tools within a CA process provides a greater degree of assurance regarding effectiveness of the controls and the accuracy of transactions, while significantly reducing audit costs, resources, and time.

Once organizations have established a solid foundation in the effective use of data analytics integrated into the audit work plan, it becomes a natural progression to begin to implement repeatable and sustainable data analytics processes and, when ready, move toward CA processes and techniques.

The following is a model data analytics process for leveraging data analytics within an internal audit project:

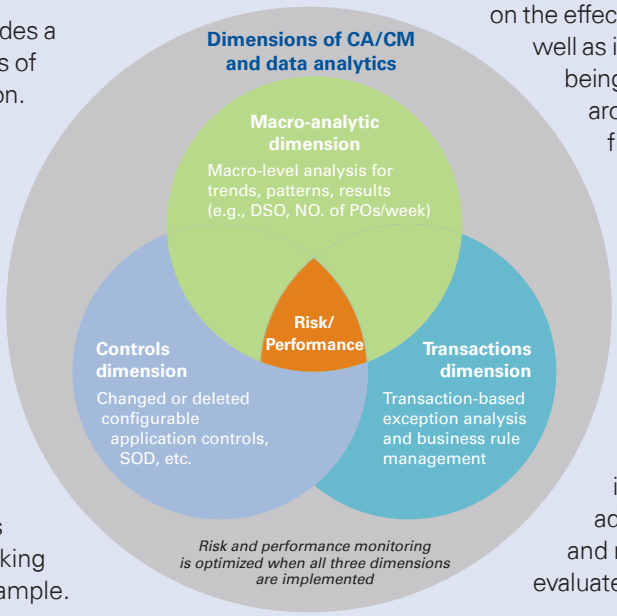
- Define the audit objective(s)
- Determine what analytics are relevant in achieving the audit objective(s)
- Design the analytics and confirm the logic
- Determine the definition of "exception"
- Identify relevant IT systems and assess availability and quality of data
- Acquire data (i.e., extract, transform, load process)
- Develop analytics (i.e., script, program, etc.)
- Run analytics and perform initial validation of results to identify data and/or logic flaws
- Confirm the results of the analytics support achieving the audit objective(s) and revise, abandon or rerun analytics as necessary
- Validate results of analytics with business owners
- Research, followup, and determine root cause of identified exceptions
- Report findings and recommendations to business owners and management
- Update analytics repository and enhance repeatability, as appropriate

Effectively integrating CA, CM, or data analytics across three dimensions

When looking to integrate CA, CM, or data analytics, there are three dimensions to consider. They include the ***macro-analytic, controls***, *and* ***transactions*** dimensions.

The **macro-analytic dimension** provides a broad perspective for effective analysis of business issues across the organization. For example, it identifies differences in key metrics to identify unusual trends, patterns, or results that may signal a larger issue that deserves a closer look.

The **controls dimension** incorporates financial controls management, segregation of duties, etc. This dimension is very effective in providing security permissions for authorized users and blocking nonauthorized users, but it is limited as it does not address issues involving authorized users making mistakes or committing fraud, for example.



The **transactions dimension** drills down to include transaction-based exception analysis and business rule management. Essentially, this dimension focuses on the effectiveness of the controls in place as well as identifying control gaps that may be being exploited (e.g., ineffective controls around vendor setup to prevent a fictitious vendor). It addresses the potential of authorized users performing unauthorized activities, regardless of if they are intentional or unintentional (i.e., waste, fraud, policy noncompliance or regulation noncompliance, etc.).

The organizational ability to leverage all three dimensions is based on a number of factors, including current IT systems, adequacy of business processes and related controls, risk areas to be evaluated, ease of implementation, and cost.

Four common scenarios for implementing CA/CM

While today's organizations are deriving greater value from their implementation of CA/CM programs, leading organizations are maturing their use of robust data analytics and combining it with their organizational knowledge of financial, operational, and compliance risks; business processes; and automated controls. Companies are also applying CA/CM techniques to identify quick wins that create return on investment and strengthen governance, risk, and compliance (GRC) while reducing operating costs and improving performance.

But, where are companies finding the most CA/CM success? In particular, there are four common scenarios present today that identify the need for, and can benefit greatly from, successful implementation of CA/CM techniques. These include:

Scenario 1

Internal Audit moves toward "repeatable and sustainable" OR expanded scopes

In this scenario, the Internal Audit department focuses on making historically performed data analytics more "repeatable and sustainable" (e.g., automating data extraction, cleansing, normalization, selected analytics, dashboard reporting, etc.), analyses and reporting activities and/or expanding the scope and coverage of existing analytics to areas not historically analyzed. For example, a company that determines that selected analytics should be performed each quarter would realize greater value by automating the ETL process (i.e., Extract, Transform, Load) and by programming and scheduling key analytics for output to a predefined set of dashboard templates that can be generated as frequently as needed.

Scenario 2

Internal Audit leverages management's systems and tools

The Internal Audit department's focus in this scenario is on connecting its data analytic tools to existing management monitoring and information systems by analyzing the output to evaluate key risk indicators (KRIs) and other trends to perform continuous risk assessment for "dynamic" audit planning purposes. For example, this may include regular adjustments to the audit plan based upon emerging areas of risk as identified by an "on-demand" risk assessment process or leveraging management's existing monitoring tools for Internal Audit department data analytics or CA purposes.

Scenario 3

Internal Audit develops and extends a pilot

In this scenario, the Internal Audit department serves as the pilot for CM processes to be extended across the enterprise on behalf of management by leveraging CM technologies for CA purposes initially, with a subsequent transition to management for their use and ownership/maintenance.

Scenario 4

Tactical or "burning platform" issue drives a CM initiative

This scenario incorporates tactical or "burning platform" issues like fraud, misconduct, and regulatory noncompliance prevention and detection. Automation of key controls or selected business processes due to a transformation or other situation drives the implementation of CM by management, frequently with the assistance of Internal Audit.

Within each of these four scenarios, Internal Audit plays a key role. The first three scenarios are Internal Audit-centric and are typically led by Internal Audit with effective teaming with key management stakeholders. The fourth scenario is typically a management-focused effort. However, it is important for Internal Audit to be connected to this effort for two reasons:

1. Internal Audit can provide value to management by contemporaneously reviewing and commenting on CM design and implementation activities
2. Internal Audit may wish to leverage management's CM process to enable a CA process, permitting Internal Audit to "continuously audit" the CM process where such an auditing effort is valuable.

Identifying common challenges

Historically, there have been a number of challenges preventing internal audit organizations from effectively leveraging data analytics and maturing to sustainable CA processes. The primary challenges we see are access to quality data and lack of understanding in how to effectively leverage data analytics in order to achieve the stated audit objective. Data analytics can be very helpful. However, data analytics will likely be unsustainable if it is applied in a stand-alone, ad hoc fashion without linkage to, or integration with, an audit work plan and the related audit objectives. For example, it may be easy to gain approval to expand a particular audit's budgeted 300 hours by 60 hours to apply data analytics on a one-time basis. However, asking the audit committee to approve a 20 percent increase in audit hours for many audits in order to incorporate the use of data analytics will likely not be approved. In addition, applying data analytics in such a fashion would not allow for the efficiency gains and/or scope expansion that many organizations are looking for through the use of data analytics.

Other common challenges, with the most common bolded, include:

General

- Determining and establishing consensus on objectives and success criteria
- Measuring and demonstrating success of efforts
- Limited resources (financial and human) to execute on a sustained basis

Data availability and quality

- **Variety of disparate information systems with different data formats**
- **Incomplete data sets; inconsistent data quality**
- Data privacy/security issues to navigate; data access may be limited

Data analytics

- **Inability to effectively leverage data analytics in order to efficiently achieve audit objectives**
- Identifying, designing, and building relevant analytics
- Establishing a definition of "exception"; addressing "false positives" and "false negatives", etc.
- Developing an efficient work flow management process around exception identification, validation, resolution; effectively managing volumes of exceptions

Change management

- Managing impact of data analytics and CA processes on people and other business processes and overcoming individual auditor's biases and preferences regarding the use of data analytics in the audit process

Moving forward with CA

As the role of Internal Audit continues to evolve, its duties expand beyond controls testing and ensuring compliance with regulations and policies. Greater expectations from management, expanding needs from the business, and increasing demands from stakeholders continue to challenge Internal Audit to drive business value by improving risk management and enhancing performance. CA can aid such efforts by producing a more efficient, more effective, and higher quality audit with better information, enabling improved decision making and strategic resource distribution to key business areas.

Whether your strategic objective is to leverage CA as a way to enhance the audit planning risk assessment process or increase the efficiency and effectiveness in the audit process, effective planning is a key to success and should involve developing an overall methodology and approach that addresses realistic expectations.

The first step in a CA initiative is to build a strategy with an effective business case to help secure top sponsorship as well as the resources needed to move forward. An effective business case can also help management understand that a CA project extends beyond tool acquisition and implementation. It can help properly define the size and scope of the project, identify the key project drivers, and identify key stakeholders.

The following steps outline a model CA development life cycle. Note that tool selection is the seventh step in the list below. Frequently, organizations make the mistake of selecting a tool before determining the strategy and key areas of focus—potentially limiting their ability to achieve their strategic objectives.

Develop a strategic plan

- Define the objectives you are trying to achieve.
- Identify key stakeholders and define the success criteria and related measurements.
- Build an effective business case.

Develop tactical plans

- Design governance and reporting structure for CA activities.
- Evaluate data analytic skills and competencies.
- Integrate data analytics into internal audit methodology and processes.
- Evaluate and select technology tools.

Design and execute implementation plans

- Manage organizational change (internal to Internal Audit and business-facing change).
- Design and deliver trainings.
- Identify focus areas for implementation of CA to satisfy strategic objectives.
- Design and establish data connection/extract, analysis, and reporting mechanisms including risk- and performance-based analytics, dashboards, scorecards, reports and alerts, etc.

Finally, if you're thinking about developing a new CA program or evaluating a program you already have in place, ask yourself these key questions. The answers will help gauge your readiness to execute your plans, or if you already have a program, it will shed light on whether your program is utilizing leading practices.

CA process – Sample leading practice questions

- Is your CA/CM process defined?
- Do your CA/CM activities assess the relationships between key economic indicators?
- Do you regularly meet with senior management and critically review management and risk information?
- Do you take into account regulatory and market developments timely?
- Is your process linked to your risk assessment and audit planning process?
- Does your process utilize technology effectively?
- Does your process lead to more efficient and effective auditing?
- Does your process assist in focusing auditing efforts on higher risk areas?
- Does your process help identify trends, patterns, and other pervasive issues?
- Are your activities documented appropriately?
- Do your activities assist in expanding coverage more efficiently?
- Do your activities assist in identifying emerging issues more quickly than traditional activities?
- Do your activities increase the detection and prevention of fraud, misconduct, and regulatory noncompliance and reduce the number of incidents?

Contact
For more information about continuous auditing and leveraging data analytics within the continuous auditing process, please contact:

Jim Littley
Principal
Global and Americas leader for CA/CM services

T: 267-256-1833
E: jlittley@kpmg.com

kpmg.com