IT Audit Perspective on Continuous Auditing/Continuous Monitoring

KPMG LLP
INTRODUCTION

New demands from the board, senior organizational leaders, and regulators are requiring IT Audit to refocus its efforts beyond regulatory and compliance matters. IT Audit is now expected to play a much larger role; one that expands its historic focus on value preservation (a controls focus) to encompass activities related to value creation (a performance focus). Some of the value creation expectations of IT Audit include:

• Focus on the C-level agenda and participation in strategy development
• Integrated risk identification and prioritization versus siloed risk management
• Evaluation of alignment of people, processes, and systems with business strategy
• Focus on defined key performance indicators
• Analysis and quantification of risk factors in new business ventures and strategies
• Understanding of shared risks among various projects and initiatives.

IT Audit is expected to offer increased synthesis and analysis of information to help management identify themes, trends, and business opportunities. Boards and their Audit Committees are seeking a “real-time” overarching view and interpretation of the control environment from IT Audit, rather than reports on individual technology areas. Increasingly, management will also rely on IT Audit to provide a conclusion on the effectiveness of the technology environment. To meet these new expectations, IT Audit will need to refine its risk assessment processes and significantly enhance its analysis of information through the use of technology.

In KPMG LLP’s (KPMG) commissioned 2009 IT Internal Audit survey,1 it was revealed that IT Audit’s powerful combination of technical and business know-how, underpinned by an understanding of operational and technology risk, can turn the function from cost center to value builder. The survey also revealed that there is a marked and encouraging shift from traditional to more proactive, value-adding activities undertaken by IT Audit. Practitioners are working more closely with IT and business functions to deliver, for instance, assurance during live projects.

To assist them in meeting the challenges of their enhanced role and increased expectations, IT Audit functions continuously seek new ways to gain access to valuable and timely information to manage risk and improve performance. Such efforts increasingly include Continuous Auditing (CA) and Continuous Monitoring (CM) of organizational processes, transactions, systems, and controls. CA/CM can free up time and create cost savings and thus allow limited audit resources to increase focus on the abovementioned value creation activities.

1 “KPMG’s 2009 IT Internal Audit Survey: The Status of IT Audit in Europe, the Middle East, and Africa.” Approximately 300 organizations from at least 20 countries participated in a 62-question survey to identify current trends in IT Internal Audit methodologies and practices.
What Is Continuous Auditing/Continuous Monitoring?

While the definitions of CA and CM may vary across organizations and industries, the goal in pursuing these disciplines is to provide greater transparency, effectively manage risk and performance, and provide continuous assurance. Depending on an individual’s role within the organization, he or she can think of CA/CM as another lens to assess or monitor the effectiveness and completeness of the organization’s Governance, Risk, and Compliance (GRC) programs, as well as to help detect control gaps, transaction anomalies, and variances from agreed-upon performance parameters or Key Performance Indicators (KPI), which is imperative to seamless business operations.

CONTINUOUS AUDITING is the collection of audit evidence and indicators by an Internal Auditor on Information Technology (IT) systems, processes, transactions, and controls on a frequent or continuous basis, throughout a period. CA efforts can provide organizations with greater audit coverage (i.e., 100 percent of the population) for the same or less effort over time — specifically by redesigning the traditional audit approach so it can become repeatable and sustainable and by retooling people, refining processes, and incorporating embedded or enabling technologies. CA allows the IT Audit team to virtually identify control breakdowns in real time (allowing action to be taken immediately) by keeping track of specific controls, transactions, and business events as they occur. The use of CA tends to raise the overall profile of IT Audit within the organization by helping identify control weaknesses that not only impact various aspects of compliance, but also areas that are imperative to effective and efficient IT and business operations.

By contrast, CONTINUOUS MONITORING is a feedback mechanism used by management to help 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 component of the control structure. CM gives management the ability to effectively monitor those areas that are most important to them, using either a control (value preservation) or performance (value creation) lens. As with CA, CM technologies provide the opportunity to change the traditional approach for management and the process owners to focus on monitoring IT and business risk and performance.

The diagram below depicts interrelationship of the three dimensions of continuous IT controls monitoring, continuous IT transaction monitoring, and macro-level analytics. Risk and performance monitoring can be enhanced when all three dimensions are implemented as it will help identify risk or opportunity for performance improvement.

“Continuous Auditing” allows the auditor to use predefined indicators to direct and focus audits in a more efficient and timely manner.
Examples include system availability, days to close service requests, or continuous vulnerability assessments.

“Continuous Monitoring” complements normal transaction processing by checking every transaction or selected transactions against prespecified criteria.
Examples include identifying transactions that exceed predefined thresholds or electronically identifying segregation of duties conflicts.

Analytical Dimension

Macro-level analysis for trends, patterns, results (e.g., TCO, system availability, etc.)

IT Control Dimension (CCM)

IT-based controls management (SOD, configurable application controls, etc.)

Risk/Performance

IT Transaction Dimension (CTM)

Transaction-based exception analysis and business rule management
Potential Benefits from Continuous Auditing

Putting the theories of Continuous Auditing into practical use can provide IT Audit an insight into areas of risk and opportunity. IT Audit can focus not only on whether a control is being performed, but also whether it is the right control and if it is being performed correctly and in a cost-effective manner. Automation can enhance the efficiency and effectiveness of the control environment so that costs can be lowered and limited resources can be deployed strategically. With CA, IT Audit is better equipped to identify and mitigate operational, external, and strategic risks associated with ERP implementations and conversions, occurrence of fraud, globalization, changes in performance and accountability, or increased legal or regulatory environment. IT Audit can test a broader range of controls by enabling automation of controls, testing, and transaction monitoring and thus expanding its audit coverage.

CA allows IT Audit to bring in ERP systems (e.g., SAP, Oracle) into their detection and monitoring capabilities and test for security, segregation of duties, and process level controls.

Furthermore, CA delivers regular insight into the status of controls and transactions across the global enterprise. Through enhanced detection and monitoring, CA delivers overall risk and control oversight capability. CA is better able to deliver the IT Audit mandate by testing a broader range of controls at a reduced cost and on a timely basis. It also allows for a greater ability to obtain more granular information when desired. While the frequency of Continuous Monitoring would likely be more real-time (e.g., daily, weekly, monthly), IT Audit may be more focused on a specific period of time or longer-term trends.

Role of IT Internal Audit in Continuous Auditing

IT Audit is in a unique position to add value and play an integral role in the successful implementation of a Continuous Auditing program. Its role should include helping establish the specifications and requirements associated with the new auditing processes and the implementation of supporting tools. For example, during an initial deployment of a CA program, IT Audit can provide knowledgeable and experienced resources to:

- Identify where the critical data resides
- Identify key control areas that are not operating consistently or where weaknesses exist
- Identify control areas that will be of key benefit/value to operational efficiency
- Drive the design of monitoring routines
- Oversee the overall implementation of the process and supporting tools.

Considering the evolving role of the IT Audit function, organizations many increasingly rely on Continuous Auditing programs (people, processes, and technologies) to help drive sustainable value preservation and integrated risk management. IT Audit can help identify risks and controls that should be monitored by CA tools, provide insight into automated controls, evaluate audit procedures and results, and continue to define and manage the process on an ongoing basis.

BENEFITS

Improved Efficiency
- Automate components of the audit program, audit tests, or review procedures and reduce wait times for data
- Audit by exception and known control gaps and deficiencies can be continuously audited
- Reduction of low value-added work and focus on high-impact areas (e.g., fraud, waste, privacy, and data security)

Enhanced Controls
- Provision of more accurate, reliable, relevant information and corrections of errors moved closer to the “source”
- Enhanced visibility of IT Audit within IT and business and improved deterrence effect
- Assistance in providing valuable insight to controls effectiveness and business process risks associated with outsourced business processes

Earlier Information
- Earlier identification and timely corrective actions of internal control deficiencies
- Improved speed of reduced surprises, such that problems do not build up
- Ability to proceed with root cause analysis for errors, policy violations, and misconduct in a more timely manner

Reduced Complexity
- Reduction of complexity through global process standardization, thereby easing the review process
- Appropriate setting and consistency of materiality thresholds, therefore reporting focus on “real issues”

Accurate Reporting
- More reliable financial reporting and ability to more efficiently report on and certify compliance with internal and regulatory requirements

...
Role of IT Internal Audit in Continuous Monitoring

Similar to its role in Continuous Auditing, IT Audit’s role in Continuous Monitoring revolves around delivering value by advising IT and the business. IT Audit can provide knowledgeable and experienced resources to advise both the business functions and IT operations on the deployment, and ongoing oversight of CM initiatives. IT Audit can help management to:

- Assess and design the overall implementation plan
- Perform risk assessments and design query protocols and reports
- Assist management through the change management process
- Evaluate software tools and provide recommendations
- Provide recommendations on reporting and dashboards
- Develop and deliver training
- Execute continuous audits.

Once management has a continuous monitoring program in place, IT Audit can continue to provide cross-functional oversight and resources in the areas of risks and controls, IT operations, business process, regulatory compliance, and forensics and fraud detection, among others.

IT Audit’s deep insight into risk and controls relating to the organization’s strategy, operations, information technology, and business processes, as well as the legal and regulatory environment gives it a unique perspective to provide value-added cross-functional advisory services that will help ensure the successful implementation of a CM program.

CA/CM Tools

Advances in technology have paved the way for increased use of Continuous Auditing and Continuous Monitoring of organizational processes, transactions, systems, and controls. Technology enabled controls auditing and monitoring tools integrated into ERP solutions or built as third-party bolt-on solutions have and will continue to evolve. While product enhancements will continue and the marketplace will continue to consolidate, organizations are leveraging technologies to change how they evaluate the effectiveness of controls and monitor performance. The success of a CA/CM initiative is highly dependent upon the effective implementation and use of technology tools.

In a KPMG commissioned survey, it was determined that automated tools that could help focus audit activity and make better use of IT Audit resources are not commonly used in areas such as planning and risk and controls analysis. Despite plenty of interest in continuous auditing software, real development and rollout is lacking in many organizations. Furthermore, despite data analysis tools being most common, a breakdown of the types of tools used to support IT auditors reveals that 33 percent of organizations do not actually use data analysis or sampling tools. As these tools can help increase the reliability of audit conclusions, their absence could also undermine the impact of audit activity.

As available tools vary in form and function, organizations need to consider the capabilities and limitations of each and determine what tools best meet their immediate and future needs. It is important to identify key requirements upfront in order to effectively evaluate available options. Such evaluation may include whether the tool is capable of auditing, monitoring, and reporting of transaction data by comparing processed transaction against a set of control rules to identify exceptions; conditions relating to system access controls; changes to critical resources and data to verify that changes are appropriate and authorized; completeness and accuracy of data as it flows through various IT processes and systems; and volume and resolution of activity in suspense areas, error logs, or exception reports. Some of the available tools today do certain elements of auditing, monitoring, and reporting better than others. For example, certain tools may be more effective at identifying changes to critical resources and determining whether changes are appropriate and authorized, while other tools only monitor error logs for specific criteria.

Considerations that are essential to an effective tool selection process include:

- Automation of Control Monitoring via Workflow
- Segregation of Duties Analysis
- Automated Controls Analysis
- Multiplatform and Cross-Platform Analysis
- Privilege Attestation
- Ability to Perform Controls Monitoring and Transaction Monitoring
- ERP/IT Systems Supported
- Capability for Inbuilt Reporting/Dashboarding
- IFRS Timing and Strategy
- Technical Requirements
- Embedded vs. Extract and Analyze
- User Licensing
- Industry Specific Capabilities
- Sales Execution/Pricing
- Software Support and Upgrade Agreements
- Multilanguage Support (Non-English)
- Global vs. Regional Presence
Why KPMG?

Many different skills are required and, because CA/CM continues to evolve, organizations may not have ready access to these capabilities in-house. Working with a sourcing partner can make sense when an organization wants to establish a CA/CM program or enhance its existing capability. A partner can help the organization with assessing its current and desired states along the maturity continuum and developing an execution plan that addresses deployment challenges. Cosourcing can also help an organization gain access to business intelligence and knowledge and realize the full benefit of the latest generation of technology tools.

Appropriate CA/CM sourcing partners can offer deep industry knowledge and business acumen, broad business process and technical skills, and the potential for global efficiencies and fixed-cost savings. They can also offer a technology suite of enabling tools and supporting content, data extraction and scrubbing experience, support in tool selection, training, and change management capabilities that are critical during the implementation stage.

KPMG understands that an organization’s risk profile is fundamental to delivering CA/CM services. By assessing the risks, we are able to prioritize and direct resources to those processes that are most important to the business and ones that provide the highest amount of return on investment.

As discussed previously, proper linkage with GRC and Enterprise Risk Management (ERM) programs is essential to a successful implementation and management of CA/CM. KPMG’s extensive knowledge and experience in advising our clients on GRC, ERM, as well as Business Intelligence, Performance Improvement, and Unified Compliance, strongly positions us as leaders in helping organizations with their CA/CM initiatives. KPMG is able to assist during various stages of the implementation process including Planning, Assessment, Design, Implementation, Execution, as well as Evaluation.

With our global network of member firms, knowledge and insight, KPMG can effectively provide value-added services relating to CA/CM. Some of the examples include:

- Design and implement CA/CM approaches including risk-based:
  - Dashboards
  - Scorecards
  - Analytics (including fraud and regulatory-risk specific)
  - Reports (area and transaction based)
  - Management Protocols
    - Notification
    - Reporting
    - Response
    - Investigation

- Execute individual CA projects

- Evaluate antifraud processes that are part of the CA/CM approach

- Controls automation

- Integration with governance, risk, and compliance initiatives

- Integration with business intelligence initiatives

- Design/incorporate with more sophisticated data analysis initiatives (e.g., predictive modeling, social network analysis)

- Tool/application evaluation and recommendation

- Training

- Risk assessment/scoping
CONTACT INFORMATION

Phil Lageschulte
Partner
IT Internal Audit National Leader
312-665-5380
pjlageschulte@kpmg.com

MIDATLANTIC:
Richard E. Archer
Principal
412-232-1590
rearcher@kpmg.com

MIDWEST:
Bernard A. Wieger
Partner
816-802-5810
bwieger@kpmg.com

Robert T. Soles
Partner
312-665-2345
rsoles@kpmg.com

NORTHEAST:
Ralph Monte
Principal
973-912-4820
rmon@kpmg.com

SOUTHEAST:
Tom Pankey
Managing Director
813-301-2001
tpankey@kpmg.com

SOUTHWEST:
Shawn Lafferty
Principal
713-319-2182
slafferty@kpmg.com

WEST:
Mark A. Lundin
Partner
415-963-5493
mlund@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.