



---

# Internal Audit – Adding Value through Continuous Monitoring

**INTERNAL AUDIT LEADERS ARE ADOPTING TECHNOLOGY STRATEGIES TO SERVE AS KEY PLAYERS IN ASSURANCE AND RISK MANAGEMENT.**

## Kathleen Wilhide

The role of internal audit is under significant transformation, facing new risks and responding to new expectations. Internal audit is at the center of the most important business trends facing executive teams today - greater accountability, higher ethics, restoration of investor confidence, and formalizing risk and governance as a business objective that is every bit as important as profitability and a competitive edge. Relationships with the audit committee, management and the external auditors have all changed, impacting expectations and oversight responsibilities.

The activities of internal audit have become critical components of effective internal control and reliable financial reporting, but are quickly advancing beyond this initial scope. Today, internal audit is, and should be, a full partner in the enterprise risk management process, while maintaining its independent status. It is an unprecedented time for internal audit.

Internal audit (IA) is a fundamental element of corporate governance structures and processes with the organization, providing assurance to executive management as well as governing bodies. To this end, IA must ensure that the internal control and risk management structure of the organization is effective.

A significant challenge for executives and line management across the business is the concept of business risk. Internal audit can play a key role in defining this concept and putting in place an execution layer to manage and mitigate risk to the organization. IA is chartered not only with evaluating internal controls, but minimizing risk to acceptable levels. To this end IA must elevate their capabilities to take a major role in the identification and assessment of business risk.

Key to success in the role of risk management requires IA to strategically leverage the latest audit technology for planning, testing, monitoring and reporting as part of the



---

management and administration of the audit and risk management function. It is impossible to have insight into financial controls, fraud and operational risks in a cost effective manner without leveraging technology. While certainly IA has used audit tools in the past, the landscape is changing and IA must take a step back and educate itself on the technologies that are out there, and how they can leverage those technologies to put in place a risk management platform that supports their new risk management mandate.

## THE CONFUSING TECHNOLOGY LANDSCAPE

There are a number of technology solutions out there that claim to focus on the area of Governance, Risk and Compliance (GRC). There are solutions known as Compliance Management solutions which have core capabilities to support compliance processes such as self assessment surveys, document handling and overall visibility. Compliance management solutions support basic governance requirements from the angle of compliance evidence gathering, and may even provide structures for enterprise risk management.

A second segment in the GRC area is most frequently referred to as Continuous Controls Monitoring (CCM). These solutions monitor activities or transactions based upon business rules, but for the most part are not integrated to Compliance Management solutions, or even traditional audit solutions. The CCM solutions dominating the market to-date focus primarily on segregation of duties (SOD).

Traditional audit tools that provide audit plan management, work program execution and testing may not be integrated themselves, and cannot access critical information that is housed in GRC solutions.

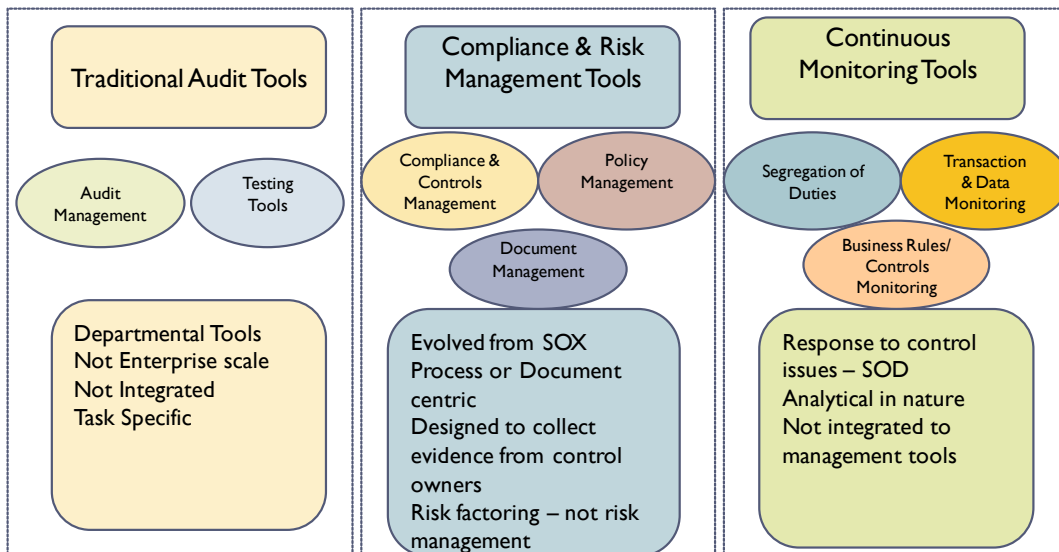
The range of GRC and audit solutions in the market today is confusing. Many do a very good job of documenting business process and internal control structures, and even providing some risk factoring for those structures. They serve as document repositories for evidence of attestation processes that are largely manual, with several layers of information gathering and employee and management reviews. In terms of automation, continuous monitoring tools serve to automate analysis processes for key controls or anomalies. In this area, SOD dominated early capabilities based upon significant weaknesses discovered in the initial phases of Sarbanes-Oxley.

Initial CCM solutions are broadening in capabilities and evolving into an area of solutions that is more appropriately called Continuous Monitoring (CM). These solutions

go beyond SOD to monitor in real time transactions or events based upon business rules that identify error, audit testing, risk monitoring or fraud identification. These applications can support processes such as compliance, audit or risk management, but traditionally have not been integrated to other solutions used to support these end to end processes. This leaves a gap in compliance, audit or risk processes.

The emerging role of IA requires these teams to look beyond the technology tools of today and determine how a strategic platform can be put in place for a more proactive assurance and risk management process. It is common for organizations to have multiple compliance and risk management and assessment processes that are performed by different groups within the company. (See Figure 1) There is a significant, strategic opportunity for internal audit to integrate those initiatives into a single risk program, leveraging and enhancing the activities that are being performed today, while elevating the risk picture to a more strategic level.

**FIGURE 1**



SOURCE: BETTER-INSIGHT 2010

Internal audit can enhance these efforts by putting in place technology for continuous monitoring, which can proactively identify risks that should be audited, or anomalies that would otherwise require significant information gathering and analysis.



---

## CONTINUOUS AUDITING VERSUS CONTINUOUS MONITORING

The Institute of Internal Auditors defines continuous auditing as a "method used by auditors to perform audit-related activities on a more continuous or continual basis." The American Institute of Certified Public Accountants has a similar viewpoint and describes continuous auditing it is "a type of auditing which produces audit results simultaneously with, or a short period of time after, the occurrence of relevant events."

As companies strive to become more proficient at managing fraud and risk while meeting compliance requirements in a cost effective manner, putting in place an integrated approach to continuous monitoring and auditing can identify issues on a timely basis, enabling companies to deal with issues on an ongoing basis as opposed to waiting until they surface in quarterly or annual audits. However, the tools that companies use today audit/test small samples of transactions and events and are not designed to support an enterprise wide continuous auditing and risk management program.

Continuous monitoring (CM) is an extension of continuous auditing, supporting broader mandates than assessing compliance controls or supporting periodic audits. Both use technologies to test and assess transactions at near real time, or 'right time' to ensure alignment with corporate controls and policies, or to identify error or potential fraud.

CM is a platform of analytic capabilities that tests all relevant transactions against a comprehensive range of business, audit and control rules, along with statistical and trend analysis to look for indications of risk and control problems. An investment in this type of platform enables a company to become 'self auditing', using technology to scan data to uncover issues and measure performance.

A CM platform supports not only traditional audits or compliance requirements for assessing controls, but performance measurement and monitoring as well. Selecting technology to support goals for continuous auditing as well as continuous monitoring makes sense, as the two processes observe essentially the same data sets. The difference is who owns the process and its purpose, with the business driving continuous monitoring requirements and audit providing value and independence through continuous auditing of the same data sets.



---

## ATTRIBUTES OF AN EFFECTIVE CONTINUOUS MONITORING SOLUTION

The following attributes are emerging as key capabilities of CM solutions:

**Comprehensive** - A solution that harmonizes all sources of information to provide a global, comprehensive and consistent view.

**Integration** - A solutions that integrates information from disparate enterprise systems but does not impact the operation of those systems.

**Content** - A solution that includes out of the box business rules based upon standard business process such as order-to-cash or procure-to-pay.

**Visibility** - A solution that delivers information in concise dashboards and reports, and facilitates drill down to the details

**Actionable** - A solution that facilitates the process of identifying issues, directing information to the right people, and provides an audit trail of actions taken and decisions made.

## SUMMARY & RECOMMENDATION

Companies will realize a return on the implementation of continuous auditing and monitoring through the timely identification of errors, fraud, and the creation of a stronger internal control environment across the enterprise. This in turn will support improvements to an organization's bottom-line results.

Internal audit is well positioned to drive these initiatives across the organization to assess the integrity of management information and to locate easy-to-miss issues. It is critical for internal audit to understand the technologies that are evolving today that can move them to the next level of detection, prevention and understanding.