Continuous Auditing/ Continuous Monitoring
Using Technology to Drive Value by Managing Risk and Improving Performance

KPMG INTERNATIONAL
Introduction

As business risks continue to proliferate, management and internal audit departments in many companies are actively seeking new ways to quickly gain access to valuable information to help manage risk and improve performance. Such efforts include continuous auditing and continuous monitoring (CA/CM) of organizational processes, transactions, systems and controls. In using CA/CM, organizations are leveraging a number of related technologies to change how they evaluate the effectiveness of controls and monitor performance—simultaneously improving their governance structures and discipline, as well as adding business value by generating better information to facilitate timely business decisions regarding risk and performance.

Advances in technology have paved the way for increased use of CA/CM. In recent years, many software vendors have developed applications that can analyze significant amounts of data on a frequent basis and provide dashboard reporting and alerts. This technology has given organizations the ability to put the theories of CA/CM into practical use by providing insight into areas of risk and opportunity.

The other development spurring the adoption of CA/CM is the ever-changing and increasingly complex business environment. The unprecedented pace of change is expected by many people to persist, so that organizations will continually be exposed to new risks, errors, fraud schemes, regulatory compliance issues and inefficiencies that can lead to financial loss and a damaged reputation.

What’s more, efforts by many companies to adopt innovative ways of assessing and managing risk and enhancing performance are now more critical than ever. Providing senior management with a post mortem after a problem has occurred is no longer acceptable. The information generated through CA/CM can change where management or the internal auditor focuses its attention and resources.

As a result, management and internal audit teams in many companies are embracing CA/CM as a range of tools that can provide efficient and continuous discipline to monitor important issues on a frequent or real-time basis, resulting in potential risks being addressed before problems arise.

This white paper seeks to define CA/CM and describes technology-enabled capabilities, how CA/CM can link to existing risk-management and operations structures, and some of the business solutions it provides for organizations today. It also considers how organizations can get started in deploying CA/CM, and offers a number of implementation considerations, including a discussion of how to build the business case for CA/CM.
Defining Foundational Concepts and How Technology Enables Them

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, CA or CM may be thought of as a lens through which he or she can assess and/or monitor the effectiveness and completeness of the organization's governance, risk and compliance (GRC) program. 1

Understanding CA and CM and how they differ is important. 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 given period. CA efforts can provide organizations with greater audit coverage (ie, 100 percent of the selected 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 internal 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 internal audit within an organization.

By contrast, continuous monitoring 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 component of the control structure.

Differentiating CA and CM

A number of key characteristics differentiate CA and CM. For example:

- CM is clearly a management monitoring function, while CA is directed at providing the internal audit department with better risk and control information.
- The level of monitoring for CM would be more granular and operational than CA, which may be more focused on key controls that provide assurance at the audit objective level.
- As its name suggests, the provision of CM is more frequent (eg, hourly, daily, weekly), while the internal audit department may be more focused on trends over time (eg, monthly, quarterly, annually).
- CM can become a key component of a company's internal control structure, and CM technologies can provide automated controls in enterprise resource planning (ERP) or general ledger environments lacking such automated controls.

Fundamentals of Monitoring

The Committee of Sponsoring Organisations (COSO) Framework makes it clear that monitoring is a timely assessment of the design and operation of controls and the taking of necessary actions.

1The governance, risk and compliance program is more than a software solution; it is a strategic discipline. GRC is a continuous process that is embedded in the culture of an organization, and governs how management identifies and protects against relevant risks, monitors and evaluates the effectiveness of internal controls, and improves operations based on learned insights. GRC is the integration of all governance, risk assessment and mitigation, and compliance and control activities to operate in synergy and balance. A GRC strategy can help create business value by reducing costs, identifying operational inefficiencies, rationalizing controls, and enabling identification and management of risks. GRC works best when multiple roles (eg, corporate secretary, corporate compliance, enterprise risk, internal audit, IT, line of business, investigations, legal) work together in a common framework of collaboration, in order to provide an overall view across governance, risk and compliance activities throughout the organization. A GRC strategy can help an organization avoid unforeseen risks, while preserving shareholder value.

Source: KPMG LLP, 2008
CM gives management the ability to effectively monitor those areas that are most important to it, using either a risk or performance lens. As with CA, CM technologies provide the opportunity to change the traditional approach of management and the process users to focus on monitoring business risk and performance. Monitoring from a process perspective is inherently a management and operations responsibility that helps provide a level of assurance that internal controls are performing as intended.² By enabling a continuous monitoring capability, CM technologies can fundamentally enhance the way internal controls are monitored, thereby improving risk management and business performance.

**Integrating CA and CM**

Neither CA nor CM needs to be present for the other to be implemented. Some organizations have successfully implemented CA without having a CM process in place; they have deployed CA to better understand risks to the enterprise, assess control effectiveness, support compliance efforts, and to manage and their internal audit resources more efficiently. Often, CA techniques can lead to management ultimately adopting such select procedures as CM.

That said, organizations that draw the maximum value from CA/CM tend to use a combination of both throughout the business. Companies that combine CA and CM effectively tend to coordinate the efforts of internal audit with management to avoid duplication of efforts and unproductive use of resources. A strong CM function can give management 20:20 vision into their operations, requiring internal audit to focus on different aspects or combinations of the risks being monitored. In this case, internal audit would need to audit the monitoring process to ascertain its effectiveness and whether management is using the CM function as intended. The context in which the metrics are designed and information received may vary according to the needs of each user.

For example, internal audit may change its resource allocation if it perceives a problematic trend forming, whereas management may want to address every problem, or exception, reported.

---

²As one of the five fundamental components of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework, monitoring is designed to “ensure that internal control continues to operate effectively.” COSO notes that “it is important that internal control is viewed as a continuous process and that effective monitoring is implemented as a component of that process—whether that control process applies to operations, compliance, or financial reporting activities.” *Internal Control—Integrated Framework Guidance on Monitoring Internal Control Systems*, discussion document, September 2007. http://www.coso.org/Publications/COSO_Monitoring%20DD_PressRelease.pdf
Integrating Tools and Analytics

Leading organizations tend to use a variety of analytic techniques across a combination of three areas of monitoring, based on a cost-benefit analysis (see Figure 1).

Figure 1
Integrating Tools and Analytics

- **Macro-Level Trends and Results Monitoring**
  (DSO,* DPO,** working capital requirements, etc.)

- **Continuous Controls Monitoring**
  (changed or deleted controls)

- **Risk/Performance**

- **Continuous Transaction Monitoring**
  (predefined business rules and exception analysis)

*Days sales outstanding  
**Days payable outstanding

Source: KPMG LLP 2008

- **Continuous Controls Monitoring.** This includes monitoring a system’s global configuration settings, access controls and rules that define how an event or transaction can be initiated, processed and recorded. An example is monitoring controls that limit access to databases holding confidential or personally identifiable information (PII).

- **Continuous Transaction Monitoring.** This includes the creation of rules and tests run against the actual flow of transactions to identify exceptions, anomalous patterns and trends, or other factors that may present risk, or are contrary to expected measures of performance, such as key performance indicators (KPIs). An example is monitoring manual journal entries for erroneous or potentially fraudulent activity, or monitoring trade accounts payable for possible violations.
• Macro-Level Trends and Results Monitoring. This relates to “seeing the forest for the trees” and requires evaluation of analyses measuring historical or emerging trends in identified risk and performance areas, thereby allowing management to link business performance with underlying changes in the organization’s people, processes and technology. Examples include trends in working-capital requirements and linkages to billing errors, inventory management issues or supply-chain inefficiencies.

The Enabling Technology Tools
Technology-enabled controls, transaction and performance monitoring tools integrated into ERP solutions or built as third-party bolt-on solutions have evolved rapidly over the years. Although product enhancements will continue and the marketplace will consolidate, these tools can provide their users the past few means to structure, document and manage business risk; monitor internal control effectiveness and performance; and detect and correct controls gaps and make performance improvement adjustments in a timely manner.

The value of such tools is in their ability to transfer a business principle into a configurable control and assess a transaction’s performance against expected results. When a configurable control or transaction does not conform to a predefined risk-based business principle, an alert is automatically generated. Such an alert could be as simple as an e-mail notification to the user and their supervisor, or a summary dashboard using control points, process area and operating unit, thus providing tactical and strategic business insights.

CA/CM brings greater insight and transparency for continuous assurance and performance. The success of CA/CM is dependent upon the effective use of technology tools. Existing technology solutions tend to have strengths in either controls or transaction monitoring, as well as types of predefined business principles and analyses. Organizations should carefully evaluate the features, functions and capabilities most appropriate for their needs before engaging a tool provider.
Linking CA/CM with Risk Management and Operations Improvement

A top-down, comprehensive approach is one way to begin a CA/CM effort. Many organizations, however, start with a business case illustrating a pilot approach to CA/CM. No matter how they choose to launch it, organizations should take steps to define the desired goal of implementing CA/CM to effectively build a and measure success. The desired result of a CA/CM initiative is not just a point-in-time assessment or an assessment of all controls on a real-time basis. Rather, the goal is an array of evaluations performed through the use of tools and manual procedures, some on a real-time basis and others on a defined frequency based on performance cycle and risk.

A key to achieving this desired result is integrating a robust enterprise risk management (ERM) program, monitoring capabilities from a CA/CM perspective, and an exception-based remediation and control improvement program (see Figure 2).

An ERM program helps the organization ensure that it designs efficient and effective controls to minimise a range of financial, regulatory, fraud, and operational risks. Such a program defines accountabilities as well as what to monitor, how, and at what frequency to monitor. Monitoring is repeatable and sustainable, a continuous process that varies based on objectives; identified risks; an organization’s size, processes and IT systems; and whether a control is automated or manual.

Based on the monitoring insights obtained, a range of exceptions or areas for improvement can be identified over time, communicated and corrected. In this way, processes can be continuously enhanced.

With a continuous process, organizations are provided with the ability to identify:
- Transactional errors across processes and business units to be monitored, reduced or eliminated
- Financial discrepancies based on misuse of funds or potential fraud and misconduct
- Regulatory compliance and workflow inefficiencies
- Performance improvement opportunities.

Managing Risk and Performance

Figure 2

Continuous Auditing/Continuous Monitoring
**Business Imperatives Driving CA/CM**

Many organizations are considering the value of CA/CM and the technology tools that enable such a program. Their efforts are driven by a number of imperatives that will also shape and influence the roadmap for CA/CM. These imperatives include:

- Complexity of the business environment
- Lack of transparency
- Increased regulatory compliance requirements
- Need for timely information to drive effective decision-making
- Technology innovations
- Increased fraud and misconduct risk
- Cost pressures
- Stakeholder expectations.

**Considering ROI**

Areas that tend to have the greatest return on investment (ROI) in an initial implementation include:

- Procure to pay
- Time and expense
- Purchasing cards (P-Cards)
- Manual journal entries
- Order to cash
- Inventory management.

**Business Imperatives**

In effect, many CA/CM business imperatives stem from two important goals: (1) to provide quality information more quickly to users (including management and the internal audit function) and (2) to improve the transparency of information offered to users concerning their areas of responsibility. In developing a CA/CM program, the key is to demonstrate clearly why these goals are important and how achieving them could drive better behavior and business results.

In making the case for better information and transparency, organizations consider the risks and the controls used to manage them. An increasingly complex regulatory environment has prompted organizations to focus heavily on issues of risk and controls in recent years. Now, as their compliance efforts become more extensive and integrated within the organization, they want to ensure they are getting business value from these efforts. A CA/CM discipline and program can help organizations integrate their efforts to address multiple requirements efficiently with tools that enable a single view of organizational risks and the controls in place to minimise them.

The portfolio of controls can be quite complex and can include manual, automated, and preventive and detective controls designed to mitigate a range of business risks by process, geography, organization unit and supporting systems. Some controls are performed on a real-time basis. Others may be performed daily, weekly, monthly, quarterly or annually.

Although CA/CM approaches are, by definition, automated, organizations will always have some level of manual control. Indeed, manual controls will always be needed in some situations (e.g., paper-based reconciliations). The key is to find a balance to make optimal use of a combination of automated and manual controls, as opportunities exist to make valuable use of both.

---

**Attributes of Effective Communication and Follow-Up**

No system can provide absolute assurance that control failures will not occur, but an effective system should be designed to identify and correct problems before they become material to the organization’s objectives. Principle 20 (“Reporting Deficiencies”) from COSO’s 2006 guidance identified three attributes that are consistent with that goal:

- **Report findings**—Findings of internal control weaknesses are reported (1) to the individual who owns the process and related controls, and who is in a position to take corrective actions, and (2) to at least one level of management above the process owner.
- **Report weaknesses**—Significant weaknesses are communicated to top management and the board or audit committees.
- **Correct problems on a timely basis**—Weaknesses reported from both internal and external sources are considered and timely corrective actions are taken.

These attributes reinforce the need for the right people to receive information such that (1) corrective action can be taken and (2) management can provide sufficient oversight to gain an understanding that the corrective action has been taken.

Source: Committee of Sponsoring Organisations, 2006
Getting Started

The first step an organization should take in its CA/CM initiative is to build a business case that will help secure support from senior management, as well as the resources to implement it.

No matter what the scope of the effort, a business case explains that a CA/CM initiative should be undertaken with the understanding that it extends beyond tool acquisition and implementation. The effort should establish a roadmap that will help link and integrate CA/CM with risk management, provide transparency into business operations and enable timely remediation of control deficiencies.

Organizations can benefit from taking the time to develop clear objectives and a good understanding of the roadmap, together with the potential obstacles, before initiating a project.

Building a Business Case

The business case for implementing CA/CM varies with each organization and depends on numerous business drivers (as presented in Figure 3).

![Figure 3: CA/CM Drivers](source: KPMG LLP, 2008)
If, for example, an organization is in the process of implementing or upgrading an ERP system, the case for improved monitoring and reporting as part of that process tends to be self-evident. An investment in CA/CM fits well in the context of a larger business intelligence initiative where CA/CM can provide critical decision-making capabilities. In many other cases, however, an incremental approach based on an ROI analysis may be more appropriate.

A key aspect of developing any business case is to clearly articulate the need or opportunity, followed by the recommended course of action. It is therefore important to identify the underlying risks that are currently not monitored, or monitored too infrequently, thereby creating undesirable exposure for the company. Such an analysis will allow the organization to build a roadmap toward the desired outcome.

Although few organizations have a mature CA/CM function, visualizing the potential of CA/CM throughout an organization is both useful and important. Most often, organizations develop a business case focused on a process or division, allowing management or internal audit to test the CA/CM concept and demonstrate to senior management its tangible and intangible benefits. When developing an initial business case, some organizations have found early success by focusing on an area they expect would benefit from deployment of CA/CM. Areas of focus are those where controls could be weak or that have a higher potential for misappropriation of assets. Such a focus on “quick wins” can result in significant savings and/or the mitigation of risks, eliminating the need to build a detailed business case for further CA/CM deployment.

A CA and/or CM implementation can be successful regardless of whether management or internal audit takes the first step. Specific efforts to properly align business objectives and risks for both types of user can allow for quick initial wins that create momentum. Over time, these programs can be further embedded in day-to-day activities.
How CA/CM can be Deployed and Measured

The following table lists some of the considerations for various potential users of CA/CM.

<table>
<thead>
<tr>
<th>User</th>
<th>Potential Requirements</th>
<th>Possible Measurements</th>
</tr>
</thead>
</table>
| Chief Financial Officer     | • Obtaining measures on risk and performance  
                                  • Rationalizing control self-assessments  
                                  • Continuous risk assessment  
                                  • Fraud and misconduct prevention  
                                  • Reduced Sarbanes-Oxley (S-O) costs  
                                  • Business continuity  
                                  • Accountability refinement | • Decreased variability in KPIs  
                                  • Results more consistent with plan/forecast  
                                  • Lower incidence fraud, reduced fraud fees  
                                  • Reduced professional fees  
                                  • Fewer audit adjustments  
                                  • Reduced S-O costs |
| Chief Information Officer   | • System performance  
                                  • Access controls  
                                  • Security  
                                  • Privacy  
                                  • Capacity  
                                  • Technology leveraging  
                                  • Business continuity | • Reduced system downtime  
                                  • Improved performance/response time  
                                  • Fewer violations of software licensing agreements  
                                  • Increased number of automated controls  
                                  • Reduced IT cost |
| Chief Audit Executive       | • Continuous risk and control assessment  
                                  • Focused audit plan  
                                  • Data integrity  
                                  • Trend identification and categorization  
                                  • Efficiently expanded coverage  
                                  • Early identification and reporting of errors non-compliance | • Improved utilization  
                                  • Reduced time to conduct risk assessment  
                                  • Reduced time required for each audit  
                                  • Reduced travel cost  
                                  • Reduced cost for bulk data analysis  
                                  • Reduced time to perform follow-up of findings  
                                  • Improved speed of reporting  
                                  • Larger percentage of audit program automated |
| Chief Compliance Officer    | • Rationalizing compliance function  
                                  • Regulatory compliance  
                                  • Reduced duplication of work  
                                  • Continuous risk assessment | • Streamlined reporting processes  
                                  • (for both internal and external purposes)  
                                  • Improved compliance statistics  
                                  • Improved ability to assign accountability  
                                  • Lower incidence of fines |

Some of the Key Implementation Considerations

Executives should consider a number of key implementation criteria when building a business case and roadmap for CA/CM. For example, the level of effort to implement a partial or fully integrated CA/CM program depends on the extent and maturity of existing monitoring capabilities.

The level of effort to expand, refine or integrate CA/CM are likely to be reduced if the controls already in place are primarily automated, and also automated tools are being used to perform certain types of data analysis by geography, process and certain key controls. Conversely, the effort to enhance a CA/CM discipline would be much greater if management’s monitoring and the internal audit function are disparate, and if an organization operates its monitoring through manual checks and balances.
To better understand its current maturity and thus the level of effort needed to achieve a partial or fully integrated CA/CM capability, an organization needs to consider certain variables for implementing or upgrading a CA/CM discipline. These variables are outlined in Figure 4, and described below.

**Figure 4**

**Assessing Maturity**

<table>
<thead>
<tr>
<th>PROCESS OPTIMIZATION</th>
<th>RISK AND CONTROLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Speed</td>
<td>• Sustained compliance</td>
</tr>
<tr>
<td>• Efficiency</td>
<td>• Operational effectiveness</td>
</tr>
<tr>
<td>• Timeliness</td>
<td>• Quality of information</td>
</tr>
<tr>
<td>• Resource allocation</td>
<td>• Transparency</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TECHNOLOGY</th>
<th>ORGANIZATION AND PEOPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Scalability</td>
<td>• Strategy and structure</td>
</tr>
<tr>
<td>• Enablement</td>
<td>• Accountability</td>
</tr>
<tr>
<td>• Cost</td>
<td>• Knowledge and skills</td>
</tr>
<tr>
<td>• Data integrity</td>
<td>• Change management</td>
</tr>
</tbody>
</table>

Source: KPMG LLP, 2008

**Process Optimization**

A strategy and implementation plan for CA/CM should be drafted, approved by management and communicated throughout the organization. Such a plan should consider the need to re-engineer processes and reallocate resources to monitor strategic risks.

Implementing CA/CM will require changes in process by both management and the internal audit function. Depending on the organization, these changes may be met with resistance. Once CA/CM is in place, individuals will receive different information than in the past. And they will probably be required to do something new or different sorts of with that information, be evaluated accordingly, and possibly even report to management in a different manner. Effective change management and appropriate, thorough executive support and communication will help organizations avoid dissatisfaction or setbacks.
Key questions to consider:
• How will the organization implement a CA/CM discipline? Will the approach be comprehensive or phased in by, for example, risk area, process, business unit, geographical area or system?
• How will the organization actively manage process improvement changes with the tools and techniques used to monitor risk and performance?
• Has the organization appropriately aligned monitoring and auditing with the respective risk and performance issues to provide the necessary transparency to enable prevention or early detection?

Risk and Controls
CA/CM is adopted to monitor the risks that could prevent an organization from achieving its objectives. A portfolio of controls should be implemented across the organization to help make compliance sustainable, and to provide data integrity and operational effectiveness.

Before significant resources are allocated to monitoring controls and transactions, management or internal audit will need to consider whether the existing controls are the most effective for addressing the underlying risks. Any appropriate changes should be made before implementing CA/CM.

In addition, leaders should give careful consideration to what should be measured, how it should be measured, where the necessary data resides, and the quality of the data. Simply making use of rules just because they exist within the technology tools without refining them could result in an unmanageable number of so-called “exceptions” or “false positives”. These in turn could result in increased inefficiencies as well as giving a false sense of security. Similarly, initiating poorly designed rules may not properly identify exceptions associated with risks and again may give a false sense of security.

Key questions to consider:
• How is risk currently managed and monitored?
• What is the driver for the CA/CM initiative—fraud and misconduct prevention, regulatory compliance or performance improvement?
• Is there agreement between management and internal audit on key risks and controls? Does the organization have a single view of financial, regulatory and operations risk?
• How robust are the change management protocols?
• Is management monitoring the right controls, and what are the tools for refining monitoring such as processes, technology and staff changes?
• How does the organization monitor performance for processes outsourced to others (eg, payroll)? Does it have access to process-specific data?
• Has the organization implemented the necessary automated controls to prevent unwarranted errors and to avoid inefficient use of resources in revising or correcting such errors if they do occur?
Technology
CA/CM must include all ERP and other financial and information management-systems the company operates so that the related transaction and configurable data can be analyzed and monitored with tools. These CA/CM tools should help detect data integrity problems, provide scalability, identify performance cost savings, as well as reducing the time taken for detection, correction and improvement.

The right technology tool is a key requirement realizing the value of CA/CM. Some organizations may find embedded tools prohibitively expensive. A careful analysis of organization-specific factors when reviewing the software requirements is important. Many software providers are willing to work with organizations to prove their value. Alternatively, some of the “extract and analyze” software solutions can assist in proving a value proposition, with some trade-offs, and are comparatively inexpensive.

Data Extract, Transform and Load (ETL) activities can be some of the most time-consuming (and frustrating) aspects of implementing CA/CM, and thus should be addressed early in the program. As with any initiative looking to improve business intelligence broadly, a CA/CM program will face challenges with comprehensiveness, accuracy, consistency and reliability of data. To begin with, data is constantly in motion, so organizations are wise to consider the timing of reporting processes. With non-integrated legacy applications, organizations may not be able to easily identify the fields in disparate databases—formats, protocols and refresh cycles can vary dramatically from system to system. Any program that relies on accurate, timely data needs to address practices and disciplines concerning enterprise data management.

Key questions to consider:
• What systems and monitoring functions currently exist and what is the workforce’s use experience of them?
• What CA/CM implementation model makes sense based on the system architecture? Does the organization use existing monitoring capabilities within the ERP system, third-party bolt-on solutions, or a combination of both? Will tools reside internally or will the organization send data to an external service provider to evaluate, detect and report exceptions and other anomalies?
• How will the tools affect the performance of business systems? Will the organization monitor with production data or a production copy? What data management practices are appropriate? How will these decisions affect monitoring real-time activity?
• What is the required frequency and sophistication of analysis? How will exceptions be reported, assigned, resolved and documented?
• What technology will be shared (or not shared) between management and internal audit?
• Has the organization considered the security and privacy requirements of implementing a CA/CM solution? How will it limit access within these tools to information on a need-to-know basis?
• What is the organization’s license cost across technologies and has it optimized this investment?
Organization and People
Organizations should have the necessary executive support for a CA/CM discipline. Management and employees should understand their roles and responsibilities and be knowledgeable on the subject. Lack of full industry and functional experience (eg, governance, risk, and compliance knowledge; fraud risk management) may create implementation barriers. Co-sourcing with an appropriate service provider may be appropriate in circumstances where there are knowledge and skill gaps (see sidebar, left).

Key questions to consider:
- Who is responsible for the CA/CM initiative, and do they have the necessary support from senior management?
- What functional knowledge (eg, fraud risk management) and skill sets exist in the workforce? What level of training will be required to deploy process and technology changes?
- How have roles and responsibilities been defined?
- Does the organization have an insight into how processes and controls function so that it can challenge the effectiveness of processes where necessary, and perform the necessary root-cause analysis for exceptions?
- How effectively does the organization manage change?

Working with a Service Provider
Continued innovation is needed if corporations are to maintain the current rate of progress in value protection and enhancement. CA/CM can work well only if the right combination of skills and resources is available. This may be difficult to achieve given the newness of these approaches and related technologies. Many different skills are required and, because CA/CM continues to evolve, organizations may not always have 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 to assess its current and desired states of capability, and to develop an execution plan that addresses deployment challenges. Co-sourcing can also help an organization gain access to business intelligence and knowledge and to benefit fully from the latest generation of technology tools. Appropriate CA/CM sourcing partners are not prevalent, but those that are experienced offer deep industry knowledge and business acumen, broad business process and technical skills, and the potential for global efficiencies and fixed-cost savings. They also offer an array of enabling tools and supporting content, data extraction and scrubbing expertise, support in tool selection, training and change management—all of which are critical during the implementation stage.
Conclusion: Measuring the Success of CA/CM

A number of indicators point to the success of a CA/CM effort. These include:

- Financial return on investment (e.g., reduction in working capital requirements through improvements to DSO, DPO, etc.; reduction in duplicate payments; reallocation of marketing expenses based on performance; and improved deployment of workforce)

- Non-financial ROI (e.g., regulatory compliance, employee compliance with policies and procedures)

- Potential to reduce reporting costs (e.g., reduction or elimination of testing procedures and rationalization of control self-assessments)

- Enhanced governance, risk mitigation, and compliance outcomes, including compliance with policies, procedures, and regulatory requirements

- Reduction in full-time equivalents or reallocation of resources to focus on significant risks

- Increased detection and prevention of fraud and misconduct

- Reduction in time required to conduct audits and investigations

- Increase in audit scope and coverage.

Implementing CA/CM is not just a technology exercise. It is a way of changing the type, speed and visibility of information on risk and performance that should have a significant impact on how business decisions are made and monitored. It takes time and attention, and a variety of challenges can be expected along the way. Organizations should ground the effort in an understanding of the extent to which CA/CM can transform their processes, risk and control procedures, technology and the approach of their workforces, building a strong case and roadmap for how to achieve its objectives.
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 endeavour 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 on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2009 KPMG International. KPMG International is a Swiss cooperative. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm. All rights reserved. KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative. Designed and produced by KPMG LLP (UK)’s Design Services.

Publication name: Continuous Auditing/Continuous Monitoring
Publication number: RRD-126843
Publication date: June 2009

Contacts

**ASPAC**
Mark Leishman  
+64 (9) 367 5939  
markleishman@kpmg.co.nz

Travis McAuliffe  
+61 (8) 9263 7271  
tmcauliffe@kpmg.com.au

Lyon Poh  
+65 6411 8899  
lpoh@kpmg.com.sg

**EMA**
Peter Paul Brouwers  
+31 40 250 2325  
brouwers.peterpaul@kpmg.nl

Jack De Raad  
+31 20 656 7774  
deraad.jack@kpmg.nl

Stephen Spellman  
+44 20 76943544  
stephen.spellman@kpmg.co.uk

**US**
Don Farineau  
+1 202 533 4320  
donfarineau@kpmg.com

Jim Littley  
+1 267 256 1833  
jlittley@kpmg.com

Deon Minnaar  
+1 212 872 5634  
deonminnaar@kpmg.com