Continuous Auditing/Continuous Monitoring

Using Technology to Drive Value by Managing Risk and Improving Performance

KPMG LLP
Introduction

As business risks of all kinds continue to proliferate, management and internal audit departments are actively seeking new ways to quickly gain access to valuable information to manage risk and improve performance. Such efforts increasingly 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 capability to put the theories of CA/CM into practical use by providing insight into areas of risk and opportunity.

The other development spurring CA/CM buy-in is the ever-changing and increasingly complex business environment. This unprecedented pace of change is expected 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 or a damaged reputation.

What’s more, management and internal audit efforts 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 are embracing CA and CM as important efforts that can provide efficient and continuous discipline to monitor important issues on a frequent or real-time basis, resulting in risk events being addressed before issues arise.

This white paper defines CA/CM and describes technology-enabled capabilities, how CA/CM links to existing risk management and operations structures, and the business capabilities it offers 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, he or she can think of CA or CM as a lens to 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 period. CA efforts can provide organizations with greater audit coverage (i.e., 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 the 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.

¹Governance, risk, and compliance is more than a software solution; it is a strategic discipline. GRC is a continuous process that is embedded into the culture of an organization and governs how management identifies and protects against relevant risks, monitors and evaluates the effectiveness of internal controls, and responds to 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 (e.g., corporate secretary, corporate compliance, enterprise risk, internal audit, IT, line of business, investigations, legal) work together in a common framework, collaboration, and architecture to bring an enterprise view across governance, risk, and compliance activities throughout the organization. A GRC strategy can help an organization prevent “surprises” while preserving shareholder value.
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 owners 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 designed. Thus, 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 better manage and utilize their internal audit resources. Often, CA techniques can lead to management ultimately adopting select procedures as CM. Organizations that draw the maximum value from CA/CM tend to use a combination of both CA and CM 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 scenario, internal audit would need to audit the monitoring (CM) 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 stakeholder. For example, internal audit may change its resource allocation if it perceives a problematic trend forming, whereas management may want to address every exception reported.

---

2 As 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](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).

These include:

- **Continuous Controls Monitoring.** This includes monitoring a system’s global configuration settings, access controls, and rules that define the parameters of 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, identifying exceptions, anomalous patterns and trends, or other outliers that represent 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 Foreign Corrupt Practices Act 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, allowing management to link business performance issues 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 over the years. While product enhancements will continue and the marketplace will consolidate, these tools provide their users the 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 the tools is in their ability to translate a business rule to a configurable control and assess transactions’ performance against expected results. When a configurable control or transaction does not conform to a predefined risk-based business rule pattern or trend, an alert can be automatically generated. Such an alert could be as simple as an e-mail notification to the business user and a supervisor, or it could be a summary dashboard by control points, process area, and operating unit, thus providing tactical and strategic business insights.

Together CA/CM brings greater insights 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 rules 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 the effort, organizations should take steps to define the desired end-state for CA/CM to effectively build a road map 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. Instead, 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 state is integrating a robust enterprise risk management (ERM) program, monitoring capabilities from a CA and a 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 and activities to mitigate a range of financial, regulatory, fraud, and operational risks. Such a program defines accountabilities as well as what to monitor, how to monitor, and at what frequency to monitor. Monitoring is a repeatable and sustainable, continuous process that varies based on objectives; identified risks; an organization’s size, processes, and complexity of IT systems; the control frequency; 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—and processes can be enhanced.

With a continuous process, organizations will have the insights 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 process workflow inefficiencies
- Performance improvement opportunities

### Business Imperatives

Ultimately, most CA/CM business imperatives stem from two important goals: (1) to provide quality information more quickly to stakeholders (including management and the internal audit function) and (2) to improve the transparency of information offered to stakeholders 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 these goals could drive better behavior and business results.

In making the case for better information and transparency, organizations consider their 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—essentially, to do more with less. 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 mitigate 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 controls. Indeed, manual controls will always be needed in some situations (e.g., paper-based reconciliations). The key is to balance the controls portfolio to make optimal use of a combination of automated and manual controls—because 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 committee.
- **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.

---

**Business Imperatives Driving CA/CM**

Many organizations are considering the value of a CA/CM discipline and the technology tools that enable such a program. Their efforts are driven by a number of business imperatives that will also shape and influence the road map 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.
Getting Started

The first step an organization should take in its CA/CM initiative is to build a business case for the effort that will help secure top sponsorship as well as resources to move forward.

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 road map that will help link and integrate CA/CM with risk management, provide transparency into business operations, and enable timely remediation of control deficiencies. Organizations benefit from taking time to develop clear objectives and a good understanding of the road map, together with the potential barriers, 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, the organization is in the process of implementing or upgrading an ERP system, the business case for implementing 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 business decision-making capabilities. In most 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 sets of risk that are currently not monitored or monitored too infrequently, thereby creating undesirable corporate exposure. Such an analysis will allow the organization to build a road map of milestones toward the desired outcome.

Although few organizations have a mature CA/CM function, visualizing the potential for use of CA/CM throughout an organization is both useful and important. Most often, organizations develop a business case for a focused process or division, allowing management or internal audit to test the CA/CM concept and demonstrate quickly to senior leadership 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. Attractive 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 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 stakeholders can allow for quick initial wins that create momentum. Over time, these programs can be further embedded into day-to-day activities.
Continuous Auditing/Continuous Monitoring

Key Implementation Considerations

Leaders should consider a number of key implementation criteria when building a business case and road map 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 would likely be less than otherwise if the controls that management or internal audit currently monitor are primarily automated and if automated tools are being used to perform certain types of data analysis by geography, process, and certain key controls. Conversely, the level of effort to enhance a CA/CM discipline would be much higher if management’s monitoring and the internal audit function are disparate and if each organization derives much of its assurance from manual checks and balances.

### How CA/CM Can Be Deployed and Measured

The following table includes considerations for potential users of CA/CM.

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

### User Potential Business Need Possible Measurements

- **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

- **Chief Information Officer**
  - System performance
  - Access controls
  - Security
  - Privacy
  - Capacity
  - Technology leveraging
  - Business continuity

- **Chief Audit Executive**
  - Continuous risk and control assessment
  - Focused audit plan
  - Data integrity
  - Trend identification and categorization
  - Efficiently expanded coverage
  - Identification and reporting of errors and noncompliance sooner

- **Chief Compliance Officer**
  - Rationalizing compliance function
  - Regulatory compliance
  - Reduced duplication of work
  - Continuous risk assessment

- **Possible Measurements**
  - Decreased variability in KPIs
  - Results more consistent with plan/forecast
  - Lower incidence of fines/fraud events, fraud fees
  - Reduced professional fees
  - Fewer audit adjustments
  - Reduced S-O costs
  - Reduced system downtime
  - Improved performance/response time
  - Fewer violations of software licensing agreements
  - Increased number of automated controls
  - Reduced IT cost of ownership
  - Improved utilization
  - Reduced time to conduct risk assessment
  - Reduced time required at each auditee
  - 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
  - Streamlined reporting processes (for both internal and external purposes)
  - Improved compliance statistics
  - Improved ability to assign accountability
  - Lower incidence of fines
To better understand its current maturity state and thus the level of effort potentially needed to achieve a partial or fully integrated CA/CM capability, the organization needs to understand certain variables that should be considered as part of implementing or upgrading a CA/CM discipline. These variables are outlined in Figure 4 and described below.

**Process Optimization**

A strategy and implementation plan for CA/CM should be drafted, approved by management, and effectively communicated throughout the organization. Such a plan should consider the need to reengineer 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 they have in the past. They will likely be required to do something new or different with that information, be evaluated accordingly, and possibly even report to management in a different manner than in the past. Effective change management efforts and appropriate, thorough executive sponsorship and communication will help organizations avoid disruptions or setbacks.

---

**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
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, geographic 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 the monitoring and auditing frequencies with the respective risk and performance issues to be monitored to provide the necessary transparency to enable prevention or early detection?

Risk and Controls

CA/CM needs to monitor the risks that would prevent the organization from achieving its objectives. A portfolio of controls should be implemented across the organization to help make compliance sustainable and 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 controls to address the underlying risks and make any appropriate changes 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 “switching on” rules that may exist within the technology tools without refining them could result in an unmanageable number of “exceptions” or “false positives” requiring attention, in turn resulting in increased inefficiencies as well as a false sense of assurance. Similarly, “switching on” poorly designed rules may not properly identify exceptions associated with risks and may result in a false sense of assurance.

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 CA and CM on key risks and controls? Does the organization have a single view of financial, regulatory, and operations risk?

• How mature are the change management protocols?

• Is management monitoring the right controls, and what is the process for refining such monitoring as processes, technology, and people change?

• How does the organization monitor performance for processes outsourced to others (e.g., payroll)? Does it have access to process-specific data?

• Has the organization implemented, to the extent practical, the necessary automated controls to prevent unwarranted errors and to avoid inefficient use of resources to rework or correct such errors?
Technology

CA/CM needs to include all ERP and other financial and information management systems the company operates so the related transaction and configurable data can be analyzed and monitored with CA/CM tools. These CA/CM tools should help detect data integrity issues, provide scalability, identify performance cost savings, and enhance cycle time for detection, correction, and improvement.

The right technology tool is a key requirement in 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 often 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 that is looking to improve business intelligence broadly, a CA/CM program will face challenges with completeness, 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 around enterprise data management.

Key questions to consider:

• What systems and monitoring functions currently exist and what is the organization’s use experience?

• 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 batch data to send to an external service provider to evaluate, detect, and report business rule exceptions and other anomalies?

• How will the tools affect the performance of business systems? Will the organization monitor against 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 has it limited 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 need to have the necessary executive support for a CA/CM discipline. Management and employees need to understand their roles and responsibilities and be knowledgeable about the subject matter. Lack of deep industry and functional expertise (e.g., 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 the sponsor (owner) of the CA/CM initiative, and does he/she have the necessary senior management support?
• What functional knowledge (e.g., fraud risk management) and skill sets exist and what level of training will be required to deploy process and technology changes?
• How have roles and responsibilities been defined?
• Does the organization have the business insight into how processes and controls function so it can appropriately challenge the effectiveness and efficiency of processes and perform the necessary root-cause analysis for exceptions?
• How effectively does the organization manage through change?

Teaming with a Service Provider

Continued innovation is needed if corporations are to maintain the rate of progress made in value protection and enhancement. CA/CM can work well only if the right combination of skills and resources is available, which is 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 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.

Co-sourcing 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 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 can also offer a technology suite of enabling tools and supporting content, data extraction and scrubbing expertise, support in tool selection, training, and change management capabilities that are critical during the implementation stage.
Conclusion: Measuring CA/CM Success

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 expense based on performance; and improved utilization of people)
- Nonfinancial ROI (e.g., regulatory compliance, employee compliance with policies and procedures)
- Potential to reduce Sarbanes-Oxley compliance 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 and reduction in the number of incidents
- 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 controls, technology, and people, building a business case and road map for how to achieve its objectives.
Contact Us
To learn more about CA/CM, please contact one of the following KPMG professionals:

**Deon Minnaar**
212-872-5634
deonminnaar@kpmg.com

**Jim Littley**
267-256-1833
jlittley@kpmg.com

**Don Farineau**
202-533-4320
dfarineau@kpmg.com
KPMG LLP, the audit, tax, and advisory firm (www.us.kpmg.com), is the U.S. member firm of KPMG International. KPMG International’s member firms have 123,000 professionals, including more than 7,100 partners, in 145 countries.

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 on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2008 KPMG LLP, a U.S. limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved. Printed in the U.S.A. KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative. 080609