Deloitte.

Continuous monitoring and continuous auditing
From idea to implementation

Continuous Monitoring and Continuous Auditing: From Idea to Implementation

Most financial and auditing executives are aware of continuous controls monitoring and continuous auditing and of the general benefits of such programs. Yet relatively few enterprises have realized their full potential, particularly at the enterprise-wide level. Deloitte sees the reason for this as twofold: first, executives have not seen a clear, strong business case for establishing either continuous monitoring (CM) or continuous auditing (CA) in their enterprises; second, they lack a clear picture of how CM or CA would be implemented in their organizations.

A quick definition, to be expanded upon below, may be in order because we have found that some confusion surrounds CM and CA. Although they are often lumped together, perhaps because they are both automated, ongoing processes, they are actually two distinct types of programs. As the name implies, continuous monitoring enables *management* to continually review business processes for adherence to and deviations from their intended levels of performance and effectiveness. Similarly, continuous auditing enables *internal audit* to continually gather from processes data that supports auditing activities.

Continuous monitoring enables *management* to continually review business processes for adherence to and deviations from their intended levels of performance and effectiveness.

The current environment of rising risks, regulatory activity, and compliance costs makes this the ideal time to consider (or to reconsider) the potential role of CM or CA, or both, in your enterprise. You might also consider what it would take to implement them, what they would look like, how they would operate, and whether to further investigate these modes of monitoring and auditing.

This paper, prepared for internal audit, accounting, financial, and risk management executives, can guide you in these considerations. CEOs, COOs, and board members who share those executives' concerns about rising risk, regulation, and costs — and the potential impact on their enterprises — may also find this paper informative.

Continuous auditing enables *internal audit* to continually gather from processes data that supports auditing activities.

As used in this document, "Deloitte" means Deloitte LLP and its subsidiaries. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

What Do CM and CA Do?

CM enables management to determine more quickly and accurately where it should be focusing attention and resources in order to improve processes, implement course corrections, address risks, or launch initiatives to better enable the enterprise to achieve its goals. CA enables internal auditors to determine more quickly and accurately where to focus attention and resources in order to better allocate audit resources and improve the quality of its audits and support of management.

CM is an automated, ongoing process that *enables management* to:

- Assess the effectiveness of controls and detect associated risk issues
- Improve business processes and activities while adhering to ethical and compliance standards
- Execute more timely quantitative and qualitative risk-related decisions
- Increase the cost-effectiveness of controls and monitoring through IT solutions

CA is an automated, ongoing process that enables *internal audit* to:

- Collect from processes, transactions, and accounts data that supports internal and external auditing activities
- Achieve more timely, less costly compliance with policies, procedures, and regulations
- Shift from cyclical or episodic reviews with limited focus to continuous, broader, more proactive reviews
- Evolve from a traditional, static annual audit plan to a more dynamic plan based on CA results
- Reduce audit costs while increasing effectiveness through IT solutions

While CM and CA need not coexist to be effective, an enterprise may maximize the value of each by implementing both because:

- Implementing CM and CA can integrate management's responsibility for the performance of controls with internal audit's responsibility for assurance regarding management's controls — while preserving audit's independence
- Increasing coordination between management and internal audit in these areas should minimize duplication of controls and efforts
- Implementing CM and CA can enable the enterprise to adapt more quickly and effectively to changes in the risk and regulatory climate

The value of CM is that it gives management greater visibility into, and more timely information on, business processes designed to achieve strategic and operational goals. The value of CA is that it enables internal audit to move from sampling accounts and transactions to coverage of 100 percent of accounts and transactions (when and where desired). Although CM and CA can be adopted separately or together, enterprises may achieve the most cost-effective development by implementing both; either simultaneously or in planned sequence.

CM and CA and Risk Management

CM and CA can improve the risk management and control activities of virtually any large enterprise. These activities have risen in importance on the agendas of many senior executives and boards, given the events of the past few years and continuing challenges in the financial and business environment. Those challenges range from heightened global competitive pressures, to more stringent regulatory regimes, to endless pressure to increase revenue and margin, to exposure to ever more aggressive forms of theft, fraud, and cybercrime.

Executives allocate resources to the initiatives they perceive as yielding the greatest return, in keeping with their organization's mission and priorities. To commit — or not to commit — resources to CM or CA executives need a clear picture of the ways in which CM and CA would enhance current risk management, control, and audit activities *and* of the ways in which implementation might proceed. This, in turn, requires that CM and CA be viewed in their proper context.

CM and CA are best considered in the context of the enterprise's overall risk management effort at the operational level. Often executives and boards consider risk management in broad terms, but have trouble bringing it down to the operational level. Yet that is where effective risk management occurs. To bring their thinking about CM and CA to operational levels, leaders can start by asking themselves:

- How do we currently monitor controls?
- How well do the enterprise's controls currently function?
- How do we currently allocate internal audit resources?
- How do we determine that this allocation is optimal?
- What costs and unintended risks do our current methods of controls monitoring and auditing create?

Such questions bring current methods of controls monitoring and auditing to light, and allow for a clearer comparison between current methods and CM and CA.

Deloitte's approach to CM and CA supports, and is supported by, the principles of the Risk Intelligent Enterprise™, which embodies Deloitte's philosophy of and approach to risk management. A risk intelligent approach departs from traditional approaches to risk management in specific ways (see sidebar, The Risk Intelligent Enterprise™). Risk intelligence provides an integrated risk management framework in which leaders and employees at all levels can recognize and manage risks in their decision-making and operating activities.

Risk intelligent practices should guide development of CM and CA systems and techniques. For instance, when contemplating CM or CA it's best to consider the full spectrum of risks across "silos," interactions among risks, and ways to build CM/CA into activities and processes. In addition, several factors in the prevailing business environment should prompt enterprises to consider implementing CM and CA. These include:

- Heightened demand for faster, better decisions and for improved, but cost-effective risk management
- Rising pressures on internal audit to provide timely assurance to stakeholders
- Increasing complexity and change in regulatory requirements
- Greater efforts to align internal audit activities with management's strategic business goals

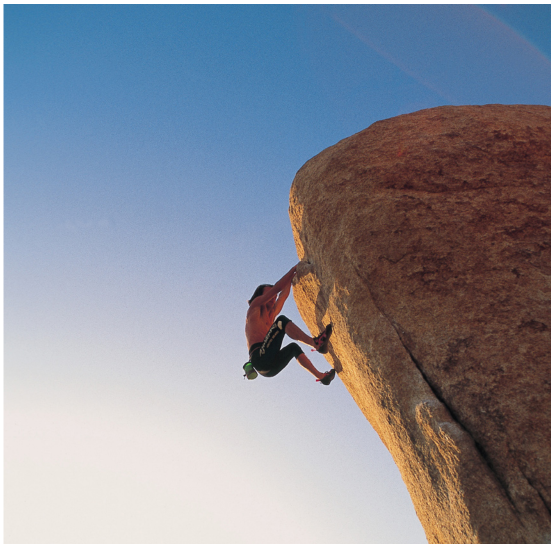
Internal audit generally does employ a risk-based approach to audit planning, and that approach can be enhanced by taking a broader view of risk and expanding audit tools and techniques. Expanding those tools and techniques to include CA, or at least some CA mechanisms, can very likely enhance internal audit's performance regardless of how risk-based its approach currently is in practice. Similarly, CM can help management to improve the allocation of risk management resources as well as risk management itself.

For example, to support the work of internal audit, CA provides information that relates to compliance with policies, procedures, and regulations, which supports financial reporting activities and goals. CM provides relevant data on processes, transactions, and accounts to management in a timely manner and at low cost, with the aim of monitoring performance and supporting decision making. Both CA and CM usually use IT-enabled tools to monitor processes, transactions, and accounts to enhance the efficiency and effectiveness of internal audit's and management's efforts.

The Risk Intelligent Enterprise™

Risk intelligence is Deloitte's philosophy of and approach to risk management, and it consists of practices that:

- Address the full spectrum of risks, including strategic, operational, compliance, reporting, security, environmental, and other risks across the enterprise
- Acknowledge the need for specialization by business and function, but also across organizational "silos"
- Consider the interaction of multiple risks rather than focusing on a single risk or event, and consider the potential impacts of multiple threats
- Create common terms and metrics for risk, and a culture in which people account for risk in every activity
- Support risk taking for reward and value creation, rather than pure risk avoidance



How would they operate?

What would CM and CA look like and how would they operate? In which situations does CM or CA have the most value? To help answer those questions, we provide a few case studies in this document, and the following brief examples of CM in action:

Transaction Monitoring

A lender wanted comfort that the pricing of each loan it extended was in keeping with its underwriting policies, in order to ensure profitability. Its practice had been to calculate loan price on a defined set of business and credit rules, but to allow manual override of these rules. However, when implemented by the lender's agents, that manual override could occur without detection, causing a potential control failure.

The solution was to continually monitor loan prices and to report deviations from the price calculated only on the basis of the business and credit rules. (Any significant deviation is now detected and reported, and exceptions are investigated and resolved.)

Controlling Freight Costs

An operating manager needed to detect unnecessary freight payments, which were set by the trucking company per the weight of the goods being shipped. The contract between the enterprise and the trucking company included clauses that guaranteed a minimum payment if the weight of a delivery fell short of the truck's maximum load. Generally, the minimum cost was set at 60 percent of the cost of a truck's maximum load. Thus, the manager needed to ascertain when trucks were being loaded at less than 60 percent of the vehicle's capacity, situations that would represent inefficiency and excess costs.

The solution was to automatically identify and report trucks that had been loaded at less than 60 percent of capacity on the same route or destination within a given period of time.

Limiting Breaches of Authority

A comptroller wanted to be able to detect limit-of-authority breaches in areas such as purchases, payables, and sales discounts. The enterprise had established systemic preventive controls to support approval levels in some processes, but those controls could be circumvented. For example, if a person authorized to sign for individual purchases of up to €2,000 wanted to approve a purchase of €10,000, he could input and approve five purchase orders for €2,000 for the same supplier and thus complete the transaction.

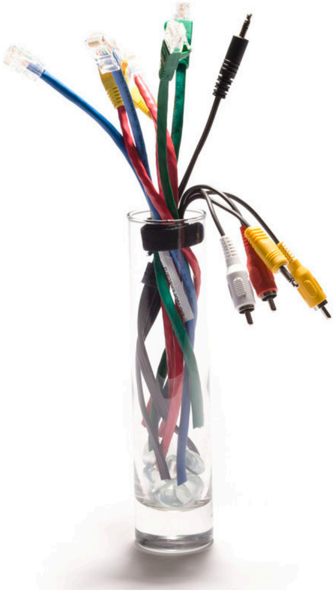
The solution was to continually monitor approvals of expenditures or disbursements to the same entity by each individual with spending authority and to compare the individual and total amounts authorized for a specific entity in a specific period, such as one day or five business days.

Personal Password Protection

A chief information officer wanted to protect passwords and detect situations in which users shared their passwords with co-workers or other parties. System security policies stipulated that system access was limited to individuals with authorized user login and password information, yet breaches had been occurring.

The solution was to automatically identify users sharing login information and passwords by detecting access by parties who had not entered the premises (as recorded by identification card swipes), concurrent use of the same login and password information at different computers, and other anomalies in instances of access.

As these brief examples show, CM or CA can be applied selectively and in targeted ways. This enables management or internal audit to experiment, gain experience, and realize early, and then incremental, returns. That said, the Risk Intelligent Enterprise™ will recognize the interconnectedness of processes and of risks and consider other areas that could be affected by each CM or CA change or initiative. The greatest benefits accrue to enterprises that coordinate CM or CA initiatives to maximize the use of automated control and audit mechanisms. The key however, is to view CM and CA in a risk management context (see sidebar, Case Study #1).



Case Study #1: European Conglomerate

Using CM in a Risk Management Context

The Situation:

An EU-based Fortune 50 conglomerate experienced several high-profile control failures that led to substantial fines and damage to reputation. Management realized that controls needed to be much more effective, particularly in purchases and payments. Key issues included a lack of a structured approach to assessing risks in these activities, loose controls in areas such as segregation of duties, and a need for robust but cost-efficient monitoring.

The Solution:

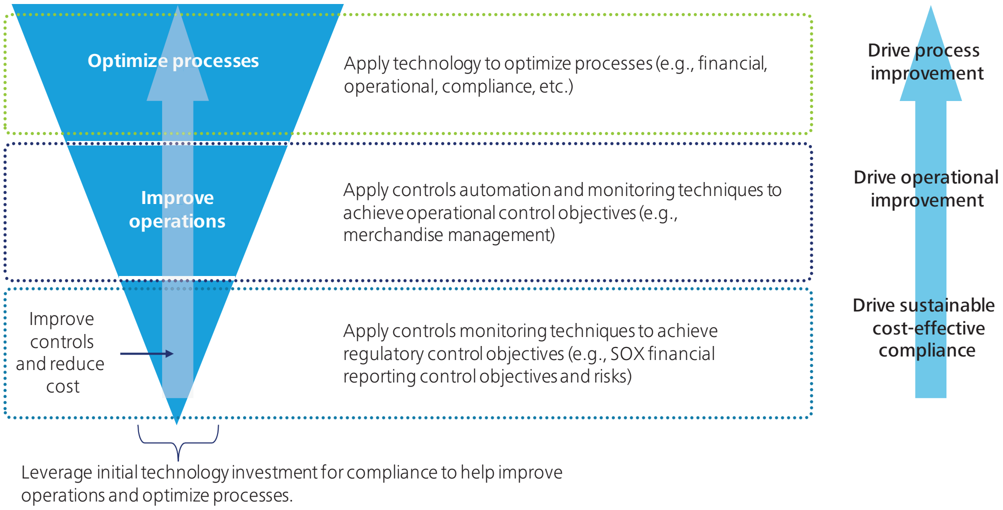
Based on the level of associated risk, Deloitte helped management prioritize the activities, access privileges, and preventative application controls on which to focus. On this basis, we developed a framework of rules to use to interrogate historic transactions, master-data changes, access-right modifications, system configurations, and user activity. This enabled us to give management the tools to identify inappropriate changes in access rights and system configurations, as well as user activity after such changes.

Via automated data extraction, we collated disparate data sets into a structured central repository. This enabled analysis of data that resided in existing systems, but had not been analyzed in light of control objectives. We worked with the enterprise to identify any significant false positives and to fine tune the rule set to help ensure that only high-risk activity was flagged for further investigation. We also recommended process of timely, appropriate, local remediation of exceptions be put in place.

To provide a practical reporting mechanism, Deloitte custom designed a dashboard to provide both a high-level and detailed view of exceptions and remediation efforts. This dashboard provided a central view of the businesses with the most and least exceptions and those that failed to investigate exceptions in a timely manner. The dashboard indicated the business units' performance, and the value or potential impact of exceptions. The latter enabled a risk-based approach to focusing identification and remediation efforts.

Developing the Business Case

Exhibit 1 — Moving CM up the value chain


Optimize processes
Apply technology to optimize processes (e.g., financial, operational, compliance, etc.)
Improve operations
Apply controls automation and monitoring techniques to achieve operational control objectives (e.g., merchandise management)
Improve controls and reduce cost
Apply controls monitoring techniques to achieve regulatory control objectives (e.g., SOX financial reporting control objectives and risks)
Leverage initial technology investment for compliance to help improve operations and optimize processes.
Drive process improvement
Drive operational improvement
Drive sustainable cost-effective compliance

In many risk management initiatives, costs can appear more certain than benefits. That's because the costs are specific near-term outlays and risks are more indistinct, longer-term, potential events. Thus, the business case for CM or CA can be difficult to make in traditional, ROI-based, monetary terms. But risks are real and that case can be made, particularly for specific activities and processes. For example, automating controls can reduce incidents of duplicate payments, internal fraud, inappropriate warranty claims, unauthorized discounts, and underperformance by service providers. The monetary losses due to future incidents, after adoption of controls, can be compared with those of past incidents.

In addition, a significant CM or CA initiative can (and arguably should) harmonize, rationalize, and optimize controls. This process can eliminate redundant controls, help institute needed controls, close control gaps, and eliminate needless reports. The savings in reduced loss, audit, administrative, and report generation and review costs can all be calculated.

Perhaps most importantly, CM can enable management to achieve financial and operational control objectives while exploiting new process-improvement opportunities. The enterprise can in that way use CM to move up the value chain (see Exhibit 1).

The three stages of CM adoption depicted in Exhibit 1 accomplish the following:

1. Initially, the enterprise uses controls monitoring techniques to *achieve regulatory control objectives*, such as those related to Sarbanes-Oxley (SOX) financial reporting and risk management objectives. This reduces costs.
2. Then, the enterprise applies controls automation and monitoring techniques to *achieve operational control objectives*, such as inventory, receivables, payables, credit, or warranty claims management.
3. Finally, the enterprise applies technology *to optimize processes*, including operational, compliance, financial, risk management, and other processes.

Generally, it makes sense first to improve controls and reduce costs, then to improve operations, then to optimize processes. This movement up the value chain helps to make the business case at each level. It also casts a CM or CA effort as a process improvement, rather than "policing" initiative, and helps in defining short-, intermediate-, and long-term goals.

Exhibit 2 — Moving along the continuum

Manually Based Processes & Controls		Technology-Enabled Processes & Controls	
Start ➔	Manual ➔	Automated ➔	Automated Controls Monitoring
Not risk-based	Risk-based approach	Application-based process controls	Automation of control testing
Redundant controls	Rationalized controls	User access & SOD controls	Continuous controls monitoring
Manual business and IT processes & controls	Management platform	Efficient testing of controls	Operational improvement
Inefficient testing	Manually intensive testing procedures	Some automated testing capabilities	Sustainable compliance processes
Reactive approach to control issues	Testing requires large samples	Testing requires smaller samples	Proactive approach to control issues
Inefficient, ineffective controls	Suboptimal controls	Effective, efficient controls	Measurable ROI & business value

From Manual to Automated

Development also occurs along a continuum defined by migration from nonexistent or manual processes and controls to IT-enabled processes and controls (see Exhibit 2). In most situations, to the extent that controls can be automated and to the extent justified by cost-benefit analyses, they generally should be. Though broad, this high-level view recognizes that many decisions arise regarding what should be controlled, how it should be controlled, and which monitoring solutions should be implemented. The latter can include IT-enabled dashboards, manual review of exception reports, and real-time approval of transactions. In general, however, movement from reliance on manual monitoring processes to automated processes is usually preferred (see sidebar, Case Study #2).

Case Study #2: Television Broadcaster

CM &Transaction Monitoring/Expense Control

The Situation:

The Shared Services group of a fast-growing global provider of cable television news and entertainment programming faced skyrocketing travel and entertainment (T&E) transaction volume. Given the company's resource limitations, both that volume and time-consuming manual audits of expense claims potentially increased the risk of error, fraud, and misuse within the T&E reimbursement process. The enterprise needed assistance in scoping, planning, configuring, and implementing its Audit Command Language (ACL) continuous controls monitoring (CCM) tools.

The Solution:

As in many business processes, moving from a manual to an automated review system involves data analytics. Data analytics assist in auditing and risk management and in testing controls and control overrides. For example, data analytics can be used to test a population of transactions, as in this instance T&E claims, so that no overrides occur without proper approval. In this case, Deloitte helped provide a suite of automated, customizable analytics for T&E expense processing, control, and audit. This system enables monitoring of T&E transactions and claims with the aim of identifying suspicious activity, errors, and exceptions.

The Shared Services group can now monitor T&E transactions on a continuous basis. The group also moved from employing a random sample approach to a more focused approach of reviewing claims that display attributes of potentially fraudulent or erroneous expenses. Using nearly real-time CM, analysts can investigate and resolve issues that might otherwise go undetected. In addition to containing costs and minimizing losses, the CCM tool provides additional assurance around compliance relating to T&E business processes.

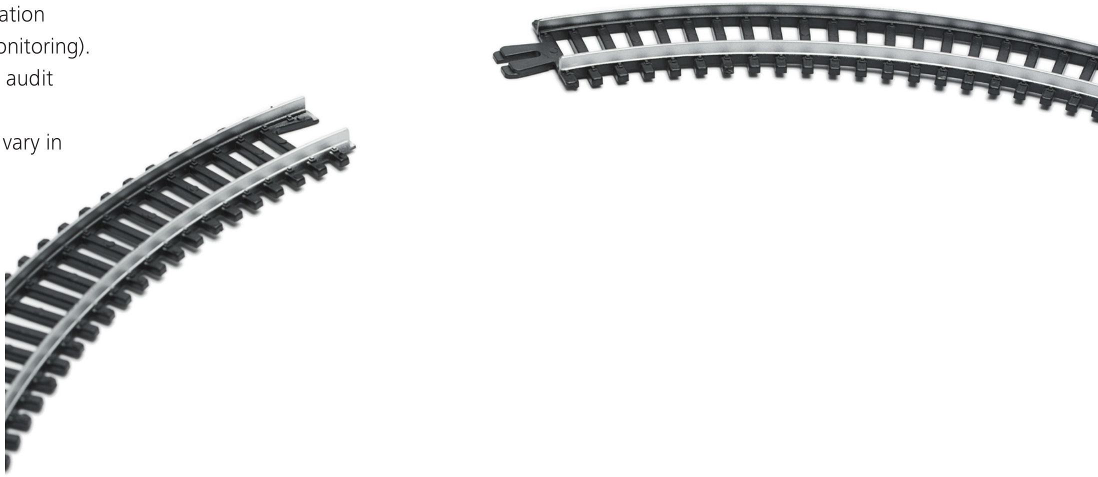
Barriers to CM and CA Adoption

Despite the potential benefits of CM and CA, barriers to adoption exist in many enterprises. Common ones include misunderstanding CM and CA and implementation issues, particularly the IT dimensions. The latter can include confusion regarding the efficacy of ERP and GRC systems, and the fit of CM or CA with such systems. Other obstacles arise in the form of internal competition for resources and funds. Often, until a risk event occurs or internal audit buckles under its workload, CM and CA can appear as "nice but not necessary."

Barriers also arise in the following areas:

- *Perceived impact on the enterprise:* CM or CA impact internal audit and other areas of the enterprise. In particular, the impact on internal audit — on its costs, head count, audit plans, workload, quality of audits, and stakeholder satisfaction — should be considered. So should the impact on the IT function and business units, and on operating, decision-making, and risk-management processes.
- *Priority of implementation:* Implementation is best planned in the context of an overall risk management framework. A method of prioritizing controls and audit activities for automation should be developed based on factors such as risk rankings, importance of audit evidence, return on investment, and ease of implementation.
- *Internal audit's readiness to develop and adopt CA:* Various audit functions vary in their readiness for CA, depending on the enterprise's lifecycle, audit focus (rotational or risk based), and use of automation (automated workpapers versus real-time monitoring). Generally, the more progressive the internal audit function, the more readily it may adopt CA.
- *IT and software considerations:* Enterprises vary in their experience and success with IT-based ERP or GRC systems. These two factors — experience and success — as well as the brands, configurations, and functions in which they have been deployed will affect CM and CA decisions and initiatives.
- *Realistic expectations:* CM and CA deliver clear benefits as detailed toward the end of this paper, but they are not achieved overnight. A large organization with complex systems and myriad activities and transactions needs time and commitment to realize the benefits. Again, however, it is possible to implement CM or CA in a limited area to gain experience and to realize substantial benefits.

In addition, it is useful to distinguish between the process side and the technology side of CM and CA, and to consider various perspectives from these angles.



Varying Perspectives and IT Considerations

Deloitte has found a wide range of perspectives on CM and CA in enterprises. Some internal audit functions view the matter from the process perspective. They focus on activities and transactions that might be subject to CA and on how to replace current audit data gathering mechanisms with continuous ones or on how disbursement limits or SOD might be automated. Others view the matter from the technology perspective and focus on how ERP, GRC, and third-party systems might enable CA or CM — and the potential roles of the various vendors and systems.

Other considerations center on operationalizing CM or CA — a perspective we have found that most enterprises fail to consider adequately. For instance, issues in operationalizing include whether you take a bottom-up or top-down approach. A bottom-up approach starts with the tools and technologies you have and works toward developing them into a platform. A top-down approach starts with the platform and more or less promulgates it throughout internal audit or another area initially and then, perhaps, other areas of the enterprise or even throughout the enterprise.

IT capabilities are a major consideration. Can the available technology enable desired controls, warnings, and exception reports? Are the desired CM or CA mechanisms compatible with existing or contemplated ERP systems? Can the mechanisms be implemented within ERP or GRC capabilities? Or must they be added on or programmed into these systems?

Most enterprises with ERP systems view them as integral to their processes and, in turn, view their GRC systems as integral to their ERP systems. This is a logical outgrowth of ERP systems providers acquiring risk management and compliance systems and offering them as part of a "total solution." The point is that these systems must be considered in any CM or CA design or implementation effort (see sidebar, Case Study #3)

Case Study #3: Global Durable Goods Manufacturer

CM & ERP Assessment

The Situation:

As part of its enterprise transformation initiative, a global manufacturer of durable goods planned a worldwide rollout of the next generation of its enterprise resource planning (ERP) system. This initiative aimed to "commonize" core finance and purchasing processes across global operating regions. This multi-year project to enable worldwide business processes required that security controls be reviewed and documented during the implementation lifecycle to minimize the potential for (and instances of) post-launch remediation.

The Solution:

The enterprise required a methodology for assessing pre-implementation ERP security and internal controls. Deloitte's methodology focused on internal controls in four key areas: business process controls, application security, data and interface controls, and general computer controls. This approach has been built into a repeatable, proven process for designing, building, testing, and deploying internal controls.

A controls assessment identified, documented, and assessed ERP internal control and security recommendations. This enabled the enterprise to evaluate their ERP control structure through successive phases and to drive management's control requirements into the program. The enterprise realized efficiencies as each regional launch progressed. Pre-implementation assessments established the controls baseline, supported future test plans, and provided the controls that were designed into the processes.

This pre-implementation review of security and business process controls consisted of three phases: Phase 1: Plan, define and design; Phase 2: Construct, test, and deploy; Phase 3: Execute deliver, and help provide ERP support. This initiative also called for audit-related assessments of the enterprise's segregation of duties tools and warranty claims management program.

The CM/CA Roadmap

Although there is no universal, sure-fire recipe for implementing CM or CA, there is a general template that a management team or internal audit function can use:

1. Develop the Business Case

Whether you are a CFO considering enterprise-wide CM or a chief audit executive proposing a CA initiative, you need to develop a strong business case. This entails:

- Connecting the initiative to the drivers of value, and the risks, in the business
- Identifying benefits and costs, and quantifying them when possible
- Placing CM or CA in the context of the overall GRC effort and clarifying their roles

2. Develop a Strategy for Adoption

A strategy for adoption identifies potential CM and CA initiatives and prioritizes them according to risks, benefits, costs, and ROI. This means:

- Targeting efforts based upon risk exposure, appetite, and tolerances, enterprise-wide and locally
- Identifying which areas are appropriate to pursue based on projected benefits, costs, and ROI
- Identifying how to set thresholds and monitor risks, as well as useful intervals and notification mechanisms (e.g., real-time notification versus daily check-in)
- Considering required resources and how current resources and priorities may help or hinder adoption

3. Plan the Design and Implementation

Planning a CM or CA initiative should be an iterative process, which involves:

- Determining the scope of the objectives
- Establishing roles and responsibilities
- Designing the CM or CA process and mechanisms
- Allocating resources and creating a timeline and project plan
- Setting reasonable expectations for performance
- Aligning people, processes, and IT resources

4. Build and Implement the CM or CA System

Once the resources are approved and in place, implementation is next. For successful implementation:

- Begin with relatively straightforward, low-cost, high-return projects
- Involve IT, business units, and other key stakeholders early on
- Create a sense of shared ownership of the project and the results
- Test the CM or CA system, particularly for its impact on the IT system, before actual launch and adoption
- Follow the plan, but make course corrections as needed
- Establish workable, practical (rather than "ideal") CM or CA procedures

5. Monitor Performance and Progress, and Refine as Needed

Migrate the CM or CA effort into the control or audit process as soon as possible after it demonstrates its viability and value. To ensure this happens:

- Report the results of the effort to management and all other stakeholders
- Demonstrate the value added — in monetary terms when possible (e.g., costs reduced, risks mitigated, or time saved)
- Verify by manual means that the early readings and results are accurate
- Adjust monitoring or notification mechanisms as needed, given their performance and the quality of the human interface

Pilot projects geared to testing the waters, gaining experience, or achieving early wins can be quite useful. With an early success or two, management or internal audit can revisit its priorities and make adjustments or move directly to the next priority. Also, given the potential savings and lower risks, many CM and CA initiatives can be structured as self-funding. Finally, be sure to obtain any necessary external expertise and guidance at each stage.

Value and Benefits of CM and CA

Broadly, CM and CA add value by means of improved compliance, risk management, and ability to achieve business goals. They can be instrumental in locating revenue leakage, for instance, due to customers taking unauthorized discounts, and in locating unnecessary costs, as in audits of service levels from third-party vendors. More broadly, CM and CA bring new levels of systematization and automation to monitoring controls, marshalling evidentiary audit data, and overseeing the enterprise. In that sense, CM and CA represent a natural progression in the evolution of the control environment and auditing efforts.

CM and CA give managers and auditors greater visibility into processes, activities, and transactions. The resulting visibility also generates greater transparency for directors, investors, and other stakeholders. In addition, CM and CA can each generate other specific benefits for the enterprise (see sidebar, Benefits of CM and CA).

Neither CM nor CA should be viewed as a short-term project, but rather as a commitment to a new, more systematic approach. The value and benefits are real, as are the barriers to implementation. The former can be realized and the latter managed, provided CM and CA are viewed in the context of risk management and implemented with a practical roadmap as your guide.

Benefits of CM and CA

Continuous monitoring can enable an enterprise to:

- Increase value through improved financial and operating controls
- Accelerate reporting to support more rapid decision making and business improvement
- Detect exceptions in real time to enable real-time responses
- Reduce — and ultimately minimize — ongoing compliance costs
- Replace manual preventative controls with automated detective controls
- Establish a more automated, risk-based control environment with lower labor costs
- Heighten competitive advantage and increase value to stakeholders

Continuous auditing can enable an enterprise to:

- Improve risk and control assurance, usually in the same or less time than previous approaches
- Reduce costs, including internal audit costs and costs associated with unaddressed control deficiencies
- Increase the level of risk mitigation for business risks
- Achieve a more robust, more effective auditing process
- Expand internal audit coverage with minimal (or no) incremental cost
- Shorten audit cycles
- Identify control issues in real time

Consider Continuousness

This document has highlighted the key considerations for a management team or an internal audit function considering continuous monitoring or continuous auditing. It has flagged the key issues and barriers, set the matter in the context of a risk management framework, and flagged potential IT concerns.

As with every initiative, decisions about CM or CA hinge on the business case. Deloitte believes that, although the business case warrants careful development, it will often be strong for CM and CA initiatives. This is particularly so in light of rising compliance, financial, operational, and other risks, and increasing demands on internal audit and risk management resources.

Contacts

To learn more about how Deloitte professionals can help you and your organization, please contact:

John Peirson
US Managing Partner
Internal Audit Transformation
Deloitte & Touche LLP
+1 612 397 4714
jpeirson@deloitte.com

Wayne Rose
Deputy Managing Partner
Internal Audit Transformation — Energy & Resources
Deloitte & Touche LLP
+1 214 840 7268
wrose@deloitte.com

Steve Curry
Partner
Internal Audit Transformation — Health Sciences & Government
Deloitte & Touche LLP
+1 215 405 7700
stecurry@deloitte.com

Paul Lindow
Partner
Internal Audit Transformation — Financial Services
Deloitte & Touche LLP
+ 1 415 783 4751
plindow@deloitte.com

Sandy Pundmann
Partner
Internal Audit Transformation — Technology, Media & Telecommunications
Deloitte & Touche LLP
+1 312 486 3790
spundmann@deloitte.com

Brett Sherman
Partner
Internal Audit Transformation — Consumer & Industrial Products
Deloitte & Touche LLP
+1 973 602 6364
bssherman@deloitte.com

Patty Miller
Partner
Internal Audit Transformation
Deloitte & Touche LLP
+1 415 783 4623
pkmiller@deloitte.com

Sheri Fedokovitz
Partner
Finance Operations & Controls Transformation
Deloitte & Touche LLP
+1 313 396 3394
sfedokovitz@deloitte.com

Steven Henchock
Principal
Finance Operations & Controls Transformation
Deloitte & Touche LLP
+1 404 220 1689
shenchock@deloitte.com

This Publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication