

COMPLETING THE ERM CIRCLE

The Role of Continuous Controls Monitoring



October 2011



INTRODUCTION

The Governance, Risk and Compliance (GRC) profession has evolved steadily over the past decade involving established concepts such as Enterprise Risk Management (ERM) and some relatively newer ones like Continuous Controls Monitoring (CCM). ERM has added tremendous value to organizations by strengthening their internal control systems. CCM helps companies to improve operational performance and lower compliance costs, according to researchers like Gartner.

As other aspects of the GRC space consolidates, are there potential synergies between ERM and CCM? This paper explores the specific challenges of achieving effective monitoring in the ERM framework and identifies CCM as a potential solution that can be used to overcome them.

WHAT IS ERM?

In 2000, the Institute of Internal Auditors Research Foundation study called, "Enterprise Risk Management: Trends and Emerging Practices" predicted:

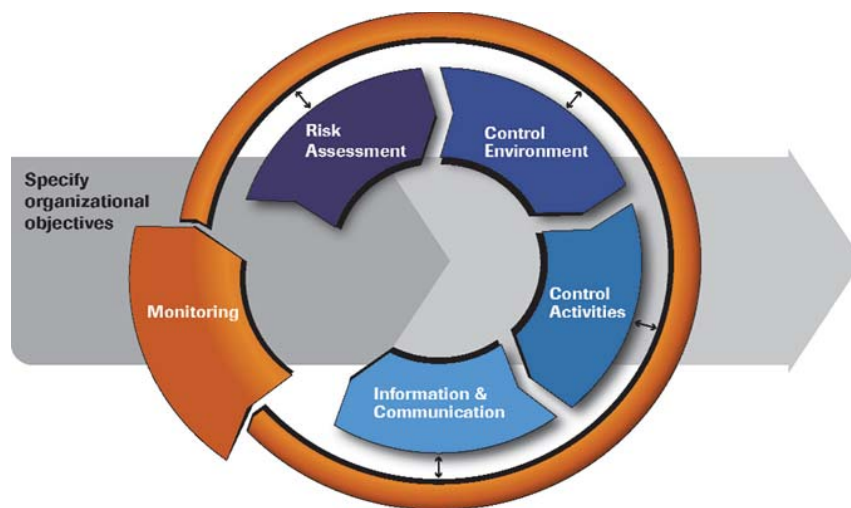
- the increasing role of risk management in the strategic planning process,
- the influence of risk management on how organisations are structured, and
- the rise in significance of the Chief Risk Officer.

Corporate practices over the last 5 years have shown these predictions to be accurate as ERM is now a consistent part of the boardroom agenda, not a passing fad.

The generally accepted definition of ERM is the process of identifying, assessing, measuring and monitoring

operational and strategic risks, while turning risks into opportunities. The importance of the monitoring element, has been entrenched in the COSO ERM Integrated Framework, where it has been assigned an entire section of the COSO cube. Additionally, the newly formed ISO 31000 standards that deal with risk management also speak to the importance of risks being monitored and addressed.

While most will agree that there have been varying degrees of success in implementing all elements of the ERM framework, one key element that remains elusive is an effective monitoring mechanism. A mechanism that not only monitors an entity's significant risks, but reports, investigates and escalates in a timely fashion, throughout the organisation.



2009 COSO Guidance - effective controls systems must include monitoring

WHAT IS CCM?

CCM is technology used to monitor controls in business processes to detect potential breakdowns and through alert mechanisms, trigger appropriate remediation activities to manage the risks. Through actively monitoring controls, this technique allows organizations to:

1. Lower compliance costs by reducing the level of manual testing.
2. Improve governance by increasing the reliability of controls.
3. Improve operational performance by automating many manual tasks to verify the effectiveness of controls.

CCM implementations vary in their level of success, as is customary for technologies in an emerging space.

However, the successful implementations produce a massive return on investment (ROI) primarily by allowing business process owners to sustain high levels of effective internal controls. This drives value by safeguarding the company's financial assets while allowing management to focus on strategic and operational activities and minimising expenditures on tedious and costly audit processes.

Organizations with successful CCM implementations will often allude to the financial gains or safeguards. However what is common in these implementations is a higher level of assurance that internal controls are operating effectively. Note that CCM technologies by themselves cannot provide complete assurances but they play a critical role in having a sustainable internal control environment.

ERM CONTROLS EVALUATION AND MONITORING

The leading ERM methodologies require senior management to ensure that there is an ongoing process of monitoring high risk activities. Specifically, the COSO ERM Integrated Framework, states that ongoing monitoring should occur in the normal course of management's activities.

Much of this monitoring effort invariably takes one or more of the following traditional forms:

- Control self assessments
- Management reports
- Key performance indicators (KPIs)

The reality is that many organisations, whether they have formally attempted to implement an ERM program or not, struggle with traditional methods of monitoring risks. They find it difficult to ensure that the right information about key risk activities is generated at the right time, delivered to the right people and that the appropriate actions are taken. In recent years the news has been dominated by major risk management failures such as BP, Societ e G en erale, Enron, and MCI World Com, which highlight this struggle.

MONITORING CHALLENGES

Control Self Assessments

- **Time taken to Perform Self Assessments**

The time frame in which the self assessments must be completed depends on the company's risk appetite, but in practice it ranges from monthly to every six months. The greater the frequency of reporting, the greater the challenge.

One of the biggest challenges is the time required by risk owners to ensure that significant automated controls are in fact working. For example, a mortgage company has a risk of losing millions of dollars where penalty charges on late mortgage payments are not being properly calculated and booked to the mortgagors' accounts.

Control Self Assessments (Continued)

The risk owner now has the challenge of selecting a sample of late payments from a past period, and testing the controls manually, or with the assistance of a spreadsheet application. Note that all of this has to be done while the risk owner continues to perform his or her normal operational activities. This has proven to be extremely difficult. The implication is that either the self assessment process or the normal daily activities suffers.

- **Delays in Detecting Breaches**

There is a delay between when a breach occurs and when it is identified. Testing the rules discussed above regarding late mortgage payments from a past period is useful but does not address the issue of potential losses because of the delay in detecting the problem.

- **Coordination with the IT Department**

Risk owners will sometimes request data from IT to upload to local spreadsheets for testing. A process that must be repeated each time a different automated test is required. This introduces data security risks as large volumes of sensitive data become resident on local computers which may not be properly secured.

- **Transparency in Reporting**

Once the relevant self assessment tests have been performed, the results are not always thoroughly investigated and/or reported to the Board or Audit Committee where serious breaches have been detected. Managers face a significant ethical dilemma as reporting serious breaches may reflect negatively on their performance and could also affect incentive payments and job security.

Managers are caught between the proverbial rock and a hard place as reporting serious breaches may reflect negatively upon their performance and could also affect incentive payments and job security.

Use of Management Reports

Management reports are sometimes outdated and lack the detail required to give managers information needed to monitor the risks they own. The root cause is often that the data management systems have not kept pace with the changing needs of the business. Managers therefore spend many hours recruiting University interns and summer workers to manually compile information for management decision making.

Key Performance Indicators (KPI)

Use of KPIs has become very fashionable, especially with the rise of performance management systems such as the Balanced ScoreCard. Again, companies have been known to recruit staff whose job is to manually compile or copy and paste data from various systems to calculate the actual performance of a particular KPI. The information generated for actual performance may contain errors, and more importantly is usually generated long after events occurred.

OVERCOMING ERM CHALLENGES WITH CCM

Control Self Assessments

- **Time taken to Perform Self Assessments**

CCM is implemented as an independent testing mechanism whereby controls are assessed by examining the core application's data. This data analysis is geared towards identifying symptoms that a control breach is imminent or has just occurred.

This is fully automated and Management only needs to react to the control exceptions but more importantly the adequacy of the control is being determined independently. Therefore, the impact on management's operational tasks is minimized as the CCM results are being managed largely by exception.

Testing of controls in a CCM environment requires some initial effort in configuration but once it is working there is minimal work in maintaining it. Unlike traditional approaches whereby there is significant work every 3 or 6 months, CCM has its efforts concentrated in the initial implementation. Additional controls can be introduced with minimal cost/effort as the corporate risk management strategy evolves. Such scalability is not available in traditional approaches to assessing controls.

- **Delays in Detecting Breaches**

With CCM, the controls may be tested several times per day, daily, weekly, monthly and so on. If a control breach takes 2 days to impact the company then examining it daily gives management another day to prevent the business from being impacted. Waiting months to know the state of a control is simply not acceptable after the investment in time and resources to implement a thorough ERM programme. The UBS multibillion loss in September 2011 is a perfect example.

- **Coordination with the IT Department**

CCM addresses major concerns regarding the safeguarding of IT assets; primarily data. The entire data extraction, consolidation and control assessment is done in a secured environment. Even the remediation process performed by management is stored in a secured database.

The recurring demands on the IT department to provide reports for risk owners to determine the adequacy of control is time consuming as noted in

the ERM framework section above but with CCM this process is implemented once and then automated. Management is only notified if there is a problem or a potential problem.

- **Transparency in Reporting**

Remediation of controls breaches is just as important as detecting them initially. Risk, compliance and audit professionals sometimes forget that the reason for designing and implementing a risk management and controls framework is to achieve corporate objectives.

The CCM framework ensures that once the issue is detected it is assigned to the relevant person, timelines are established and an escalation path determined. Other critical players are also notified such as Internal Audit, Risk and Compliance. There is no opportunity for the issue to be concealed and therefore all stakeholders are inclined to collaborate and resolve the breakdown in control.

A transparent accountability process is one of the biggest benefits of implementing a CCM solution in support of ERM. For example, if a mortgage has been issued outside the acceptable interest rate bands in a financial institution the objective is not simply to find the problem; it has to be resolved. A CCM solution is configured to detect the issue and manage its resolution including verification that the interest rate has been adjusted or that management accepted the non-compliance.

Use of Management Reports

Within a CCM framework the management reports are based on the entire data set, not just a sample which may or may not be representative of the actual business processes in place. Report creation can be automated at any desired frequency to provide accurate assessment of overall performance, allowing for informed decisions as trends develop.

Key Performance Indicators (KPI)

KPIs can be measured more frequently and accurately than available in the traditional ERM environment given that the data input required would be automatically extracted and processed by the CCM tool. The foregoing will therefore enhance the accuracy of KPIs and the speed of their generation.

ROLE OF INTERNAL AUDIT

Audit's Brand Enhancement

Given that there would be more efficient ongoing monitoring, both by Management and Internal Audit, using CCM will enhance the ERM environment. The power of CCM helps Management and Internal Audit to become more appreciative of each other's role. For example, in environments where management is sceptical of audit activities, but where CCM is seen as an effective audit tool to highlight major costs savings and similar efficiencies, management will be inclined to be more collaborative.

Independence

In environments, where CCM is first implemented by internal auditors (continuous auditing), the auditors' image and reputation in the organisation is significantly enhanced. This frequently results in management asking the auditors for advice and direction as they move to install their own CCM solution (continuous monitoring).

In this situation auditors must be careful that their independence is not tainted based on their close association with management's CCM implementation.

Keys to safeguarding independence include, but are not limited to:

- Ensuring that all decisions are made by Management and not Internal Audit.
- Internal Audit not voting at Risk Meetings.
- Internal Audit giving advice only and not instructions.
- Ensuring that it is clearly understood that acceptance of Audit's guidance is solely at the discretion of Management.
- Management is aware of Internal Audit's right to audit and to bring new insight into Management's CCM implementations based on changes in the risk environment.

CCM AS A STRATEGIC DRIVER

Operational risk failures have led to devastating consequences for a number of companies around the world in recent times. Failures ranging from major compliance breaches to rogue traders violating their trading limits without immediate challenges from the middle offices. In some instances, these operational failures have led to companies going out of business or requiring major capital injection by government or shareholders. The message should now be absolutely clear to Boards, Management, Audit Committees, Regulators, Internal Auditors and other stakeholders

that operational risk management is now a strategic business initiative. CCM is indeed a powerful tool that can be used to strengthen the control environment for key automated operational risks. It can be used to test and automatically report breaches in compliance rules, trading rules, and any other business risks that are deemed to be critical. All of the foregoing will therefore serve to protect the reputation of an organisation and potentially its very existence.

CONCLUSION

CCM implementations are often focused as a technology initiative without adequate grounding in risk assessment and management. Effective ERM on the other hand, must have a robust, ongoing controls monitoring mechanism that alerts management at the appearance of “things going wrong”. ERM implementations are often too dependent on human input for determining the effectiveness of internal controls.

Allowing CCM and ERM to enhance each other will solve many long standing challenges in governance, risk and compliance disciplines. ERM should be used to establish the foundation for implementing effective

internal controls monitoring, while CCM should be used as a powerful tool to provide more independent and timely information on the effectiveness of internal controls.

When implemented properly, management and other stakeholders will experience a remarkable improvement in the value added by both CCM and ERM primarily by creating a sustainable and dynamic internal controls environment.

ABOUT US

CaseWare

Founded in 1988, CaseWare is an industry leader in providing technology solutions for finance and accounting, governance, and risk and audit professionals. With over 250,000 users in 130 countries and 16 languages, CaseWare products deliver tremendous value across industries and continents.

Proven Success

Our customers include Big Four and other major accounting firms, as well as Fortune 500 and Global 500 companies. Governments with 9 of the 15 largest economies use our technologies to provide assurance on spending and taxation compliance.

A Leader in Continuous Controls Monitoring

CaseWare continues to redefine the continuous controls monitoring space with its flagship product, CaseWare Monitor, providing a simple, reliable solution for organizations.

Authors

Andrew Simpson B.Sc., MBA

Chief Operating Officer
CaseWare RCM Inc.

Bruce Scott FCCA, MBA, CIA, CISA

Partner, Risk Assurance Services
PricewaterhouseCoopers



CASEWARE

E-mail: rcminfo@caseware.com

www.caseware.com