



Completing the ERM Circle

A Role for Continuous Controls Monitoring

Andrew Simpson MBA, CISA Chief Operating Officer CaseWare RCM Inc.

Smart controls.
It's just Good Business



- Definitions
- COSO Integrated ERM Framework
- Self Assessments
- Challenges with Traditional Approaches
- CCM as a Solution
- Summary

What is ERM?



Enterprise Risk Management*

Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

^{*} Committee of Sponsoring Organizations of the Treadway Commission (COSO)

What is CCM?



Continuous Controls Monitoring

A technique used to monitor controls in business processes to detect potential breakdowns and through alert mechanisms trigger appropriate remediation activities to manage the associated risks.



- Definitions
- COSO Integrated ERM Framework
- Traditional Approaches to Assessment
- CCM as a Solution
- Role of Internal Audit
- Summary

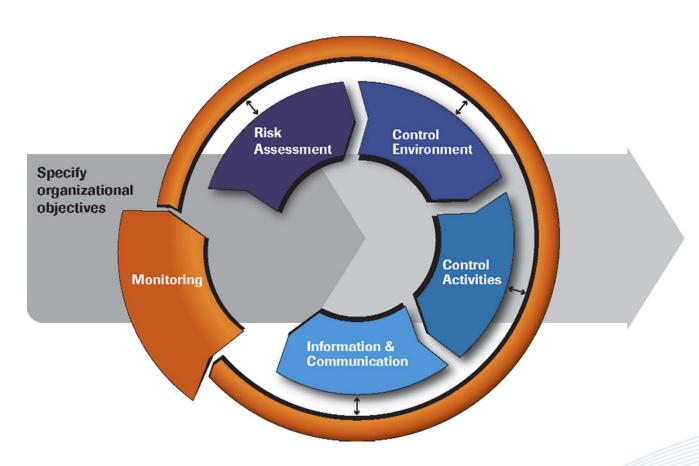
COSO ERM Framework





Importance of Monitoring





2009 COSO Guidance - effective controls systems must include monitoring



- Definitions
- COSO Integrated ERM Framework
- Traditional Approaches to Assessment
- CCM as a Solution
- Role of Internal Audit
- Summary

Traditional Monitoring



- Control Self Assessments
- Management Reporting
- Key Performance Indicators (KPI)

Challenges in Self Assessment



- Time taken to perform self assessments
- Delays in identifying control breaches
- Coordination with IT
- Independent reporting



- Definitions
- COSO Integrated ERM Framework
- Traditional Approaches to Assessment
- CCM as a Solution
- Summary

Possible Role of CCM



- Independent monitoring of automated and partially automated controls
- All the effort is in the initial design
- Continuous detection of breaches
- Transparency in detection and remediation
- Addressing IT concerns
- Collaborative approach to timely remediation

An Example



Risk: Invoices may not be valid and/or properly authorized

Control Activity: Matching invoices to goods receipt

Owner: Category Management

Method: Partially Automated

Type: Preventative

Frequency: Recurring

COSO Component: Control Activities

Risk, Control and Audit Steps



Zisk

Invoices may not be valid and/or properly authorized.

Contro

The AP Clerk matches the goods receipt form to the invoice within the system and allows for a maximum 0.5% difference.

For differences below the threshold a manual reconciliation proof sheet is created by the AP Clerk and approved and posted by the AP Supervisor to the adjustment account within the system.

Differences above the threshold are put on hold and investigated by the relevant Category Manager and the AP Clerk.

Audit Steps

Obtain a listing of all invoices for the testing period selected.

For a sample of invoices obtain the goods receipt form and re-perform the AP Clerk's reconciliation between the invoice and goods receipt form.

For all differences that fall below the threshold verify that a manual reconciliation proof sheet is created by the AP Clerk.

Verify that the manual reconciliation proof sheet is approved by the AP Supervisor.

Obtain a system printout of all adjustments and verify that the difference was posted by the AP Supervisor to the account within the system.

Verify that all differences that fall above the threshold are investigated by category management and the AP Clerk.

The CCM Component



Zisk

Invoices may not be valid and/or properly authorized.

Contro

The AP Clerk matches the goods receipt form to the invoice within the system and allows for a maximum 0.5% difference.

For differences below the threshold a manual reconciliation proof sheet is created by the AP Clerk and approved and posted by the AP Supervisor to the adjustment account within the system.

Differences above the threshold are put on hold and investigated by the relevant Category Manager and the AP Clerk.

CCM

Extract all new invoices from the system.

Compare to Goods Receipt entries in the system.

Reconcile the differences below the threshold to the adjustment account.

Assign any exceptions to the relevant Category Manager.

Assign any variances above the threshold to the relevant Category Manager.

Properties of the CCM Testing CASEWARE



Frequency: Daily

Detect: Any non-compliance over and below the threshold

Assignment: Category Management

Deadline: Resolve same day

Evidence: Due diligence performed on those over the threshold and any other exceptions detected

Value: Ensure that the control effectiveness is sustained at a high level

Benefits of this Approach



- Independence
- Efficiency and effectiveness
- Less dependency on management
- Can be integrated into operations
- Comprehensive IT solution
- Collaboration



- Definitions
- COSO Integrated ERM Framework
- Traditional Approaches to Assessment
- CCM as a Solution
- Summary

Strategic Implications



- Operational risk failures
- Strategic implications
- Capital injection
- Existence

Whitepaper



Available for Download

Authors:

Andrew Simpson

Chief Operating Officer CaseWare RCM Inc.

Bruce Scott

Partner, Risk Advisory Services PricewaterhouseCoopers

Conclusion



- ERM should influence the controls being monitored in CCM
- CCM should be used extensively in the monitoring phase of ERM

Thank You



Andrew Simpson rcminfo@caseware.com