

Continuous Controls Monitoring for Transactions: The Next Frontier for GRC Automation

French Caldwell, Paul E. Proctor

Continuous controls monitoring for transactions (CCM-T) is an emerging governance, risk and compliance (GRC) technology that monitors ERP and financial application transaction controls to improve financial governance and automate audit processes. CCM-T ensures that business rules and policies are effective, reduce compliance and audit costs, and support risk management.

Key Findings

- CCM-T can produce a quick return on investment by identifying failures of internal controls.
- CCM supports continuous monitoring (CM) and continuous audit (CA).
- CCM solutions include segregation of duties (CCM-SOD), transaction monitoring (CCM-T), master data (CCM-MD) and application configuration (CCM-AC).

Recommendations

Consider CCM-T if any of the following goals apply:

- **Lowering compliance costs** — A CCM-T solution can reduce the costs of audits by eliminating much manual sampling and minimizing the time it takes to gather documentation.
- **Improving financial governance** — CCM-T can increase the reliability of transactional controls, improve auditor trust and increase the effectiveness of anti-fraud controls.
- **Improving operational performance** — CCM-T controls such as those that monitor duplicate payments, incorrect discounts or misapplied warranties go beyond what most people consider compliance. CCM-T can improve key processes and profitability.

The following considerations are important when comparing the cost against savings and benefits:

- CCM is simplest and least expensive to apply in a homogeneous ERP environment for which the vendor has a preconfigured controls library.
- When financial processes are spread across multiple instances, and especially when there is a mix of ERP financial applications and/or other non-ERP financial applications, large amounts of customization will add significant expense. However, CCM potentially could be used to mitigate the need to move to centralized financial systems in ERP, and

costs of customization should be balanced against what it would cost to migrate to a single ERP system.

WHAT YOU NEED TO KNOW

Financial processes have many business rules and policies (that is, controls) governing transactions that are well suited for automation. ERP financial applications enable automation of controls, but not their automated monitoring. CCM technologies are applied automatically and periodically to monitor the automated controls for processes that are repeatable, consistent and predictable. CCM-T can produce a financial return on investment by identifying exceptions or failures of internal controls for transactions, which in turn may be due to operational deficiencies or control gaps.

ANALYSIS

Technology Description

Critical financial processes — such as travel expense management, order to cash and procure to pay — have many business rules or policies associated with them that address accounting, reliability and anti-fraud issues. To ensure that policies and rules are followed, many ERP and financial applications have built-in internal controls with simple gated logic (see Note 1 for an example of an internal control). However, the existence of these built-in automated controls does not ensure that they are turned on, that they are configured appropriately, and that they are not regularly overridden or bypassed — thus establishing the need for a solution that can monitor these controls.

Continuous Controls Monitoring

Continuous controls monitoring (CCM) is a set of technologies to assist the business in reducing business losses through continuous monitoring and reducing the cost of auditing through continuous audit of the controls in financial applications. CCM technologies are applied automatically and periodically to support processes that are repeatable, consistent and predictable.

CCM technologies fall within the GRC marketplace. For more information on the GRC marketplace, see "A Comparison Model for the GRC Marketplace, 2008 to 2010." CCM is a subset of a broader set of technologies called "controls automation and monitoring" (see Note 2), which includes infrastructure, systems and other application controls. They have also been referenced as "controls-monitoring analytic applications" in the broader packaged financial application market (see "Leveraging Financial Analytics").

CCM for Transactions

This research addresses CCM for transactions; however, customer requirements often require CCM solutions that have capabilities in multiple CCM subsegments. Besides CCM-T, the other subsegments are CCM for segregation of duties, CCM for master data and CCM for application configuration (see Note 3 for definitions of the subsegments).

CCM-T provides for broader visibility into all transactions, eliminating the need for manual sampling of transactions. The traditional method to monitor that policies and rules are being followed is manual sampling of transactions. However, manual sampling is labor-intensive, is expensive, lacks timeliness, represents a tiny fraction of the transactions and will often not find a singular event such as a single instance of fraud.

CCM-T solutions often are based on the same technology as audit analytics software — which is the tool used by auditors during the course of periodic audits to run either standard or ad hoc

queries against sets of transactional data. Essentially, CCM-T is audit analytics preconfigured with a set of standard queries that are run in batch mode on a frequent, near-real-time basis — often nightly.

Technology Definition

CCM-T software analyzes ERP and other financial application transactions to identify exceptions to policies, business rules and built-in application controls. CCM-T software can also be used to establish controls as well as monitor them. CCM-T software has several functions, including transaction monitoring, exception and remediation management, reporting and analytics, and workflow:

- **Transaction monitoring** functions automatically, periodically imports transaction data from ERP and financial applications, and applies a set of predefined audit analytics to identify control exceptions.
- **Exception and remediation management** supports tracking the response to identified control failures and other deficiencies, along with the process of addressing exceptions.
- **Reporting and analytics** supports trending and audit analysis, audit trails, dashboards, and the generation of reports.
- **Workflow** supports the notifications and alerts, reviews, approvals, and other process automation needs.

Uses

When implementing CCM-T, most organizations start with the procure-to-pay process. Procure to pay is a focus for anti-fraud, and it also provides an opportunity for immediate return on investment by reducing, for example, payment of duplicate invoices. Next steps can include travel and entertainment (T&E) and order-to-cash processes. CCM-T and the other CCM subsegments support both continuous monitoring for management and continuous audit for internal auditors:

- **Continuous monitoring** is a business management monitoring function used to ensure that controls operate as designed and that transactions are processed appropriately. CM uses control automation to reduce fraud and improve financial governance, typically resulting in an immediate return on investment. It improves the reliability of the controls and improves the management oversight, policy enforcement and operational efficiency for critical financial processes (see "Q&A on Financial Governance Market Trends"), often producing hard-dollar savings.
- **Continuous audit** is the periodic collection of audit evidence and indicators for the benefit of internal audit. CA reduces audit costs by automating the audit process and eliminating the cost of manual sampling. To avoid audit deficiencies, it is important that policies are being followed demonstrably and that exceptions are documented and proven to be within the boundaries of good practice.

Despite the benefits of CA and CM, too little attention has been placed by chief financial officers, internal auditors, and corporate risk management and compliance leaders on the automation of financial controls monitoring. This approach contrasts sharply with IT risk and compliance managers who invested significantly in infrastructure controls automation tools like server configuration auditing, and access controls like segregation of duties. Their objectives were to hold down compliance costs associated with manual process controls, while at the same time addressing audit findings, and in large measure, those objectives have been met. Furthermore, the Public Company Accounting Oversight Board's (PCAOB's) Audit Standard No. 5 encourages

controls automation as a means to lower audit costs and improve controls reliability (see "Sarbanes-Oxley Update: How to Best Support the CFO"). CCM-T and other CCM solutions can produce similar benefits from the automation of financial application controls monitoring.

Selection Guidelines

The following are common functional criteria to consider when selecting a CCM solution:

- **ERP Compatibility** — Is the solution compatible "out of the box" with the organization's version of the ERP financial application? Some solutions may not be compatible with older versions, and some focus on just one or two ERP vendors. If they are not compatible out of the box, then a significant amount of custom integration is required.
- **Controls Library Coverage** — Does the solution come with a predefined set of controls for your financial applications? Some vendors have controls libraries for many types and versions of ERP financial applications, while others are more limited.
- **Business Rule Engine and Analytics-Processing Capability** — Are there sufficient facilities for reducing false positives? Does the capability support the flexibility to build custom controls analytics for your environment? Organizations should also consider how often they want to run their analytics, because some products are better suited to run quarterly than in near real time.
- **Remediation Workflow** — Does it support the necessary scalability, flexibility and delegated administration to automate detection and remediation processes end to end?
- **Cross-Platform and Multiplatform Application Support** — Will the solution work for organizations that have multiple versions of ERP financial applications from multiple vendors? Can it import transactional data from all of your required applications (cross-platform)? Can it correlate transactions from multiple applications (multiplatform)?
- **Continuous Audit Support** — Does your external or statutory auditor use the same vendor for audit analytics? While this criterion should not be a major one, many organizations like to consider the CCM-T solution that is based on the audit analytics solution that their audit firm uses.

Besides these functional criteria, another major consideration is the services required to implement and tune the CCM solution. In a multi-business-unit environment where CCM is implemented across many different financial applications, customization service costs can be many times the license fee.

Technology Providers

The following are examples of vendors offering CCM-T solutions:

- **ACL Services** — ACL AuditExchange, an audit analytics product, can be customized for a CCM-T solution.
- **Oversight Systems** — The Oversight solution may be run in near real time and is also available as software as a service (SaaS). Oversight also offers audit analytics.
- **Oracle** — Oracle Transaction Controls Governor has transaction controls monitoring for Oracle and PeopleSoft financials.
- **SAP** — SAP GRC Process Control is a broad-based business process controls application that includes monitoring financial application controls, among others.

- **Approva** — Approva BizRights has transaction controls monitoring for Oracle, SAP and several other ERP applications. Approva also offers audit analytics.
- **Security Weaver** — Security Weaver Process Auditor enables transaction controls monitoring for SAP. Security Weaver also offers audit analytics for SAP environments.
- **Infogix** — Infogix Controls are a broad-based CCM solution that can be applied to transaction controls monitoring.

Some business process management and business process analysis vendors' solutions also have been used to automate transactional controls and their monitoring.

RECOMMENDED READING

"A Comparison Model for the GRC Marketplace, 2008 to 2010"

"Sarbanes-Oxley Update: How to Best Support the CFO"

"Q&A on Financial Governance Market Trends"

"Financial Governance Will Emerge to Enhance Financial Controls and Regulatory Reporting"

Acronym Key and Glossary Terms

CA	continuous audit
CM	continuous monitoring
CCM	continuous controls monitoring
CCM-AC	continuous controls monitoring for application configuration
CCM-MD	continuous controls monitoring for master data
CCM-SOD	continuous controls monitoring for segregation of duties
CCM-T	continuous controls monitoring for transactions
ERP	enterprise resource planning
GRC	governance, risk and compliance
PCAOB	Public Company Accounting Oversight Board

Note 1

Internal Controls Example

A common internal control is a "three-way match." It prevents payment for goods that have not been received, but for which the supplier has submitted an invoice. With a three-way match, the business rule logic requires that, for payment to be made, the following three items match:

- The original purchase order
- The vendor's invoice
- The receipt record for the items that were received

If the rule is not met, then the controls within the accounts payable process will block payment. The problem is that many of these automated controls are overridden — often for very good reasons, but without documentation and identification of compensating controls. For instance, perhaps it is common for an in-house supplier not to submit an invoice, but instead an inventory record is reconciled with receipts monthly — but payment is made on receipt. If the three-way match is turned off for this legitimate exception, then it could open a path for fraud. Over time, the exceptions can proliferate and become the norm.

Note 2

Controls Automation and Monitoring

Controls automation and monitoring, as defined in "Hype Cycle for Governance, Risk and Compliance Technologies, 2008," act proactively to implement controls through business rules or reactively to monitor controls through analysis of processes, transactions and events. Controls automation and monitoring can take many forms and operate at several levels of the enterprise architecture. At the infrastructure level, controls automation and monitoring focus on configuration management and network access. At the system level, they focus on identification and access. At the application level, they focus on segregation of duties and, most recently, on rules governing transactions and behavior.

Note 3

Continuous Controls Monitoring

There are four technologies that make up CCM:

- **CCM for Segregation of Duties (CCM-SOD)** — Used to manage a number of access conflicts present in ERP and financial applications. See "MarketScope for Segregation of Duty Controls Within ERP and Financial Applications."
- **CCM for Transactions (CCM-T)** — Used to continuously monitor ERP and financial application transaction information to improve governance and automate audit processes. CCM-T is the focus of this note.
- **CCM for Master Data (CCM-MD)** — Automates controls related to ERP and financial application data. It is an element of many data quality products. See "Magic Quadrant for Data Quality Tools."
- **CCM for Application Configuration (CCM-AC)** — Used to monitor the presence, appropriate configuration and modification of built-in application controls. CCM-AC is used in conjunction with each of the other three CCM technologies.

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509