Continuous Monitoring: Match Your Business Needs with the Right Technique

Jamie Levitt, PwC
Ron Risinger, PwC

September 11, 2012
Agenda

1. Introduction
2. Challenge
3. Continuous Monitoring
4. SAP’s Continuous Monitoring Tools
5. The Continuous Monitoring Roadmap
The purpose of this presentation is to give you an understanding of how:

- Continuous monitoring techniques such as continuous transaction monitoring (CTM) and continuous control monitoring (CCM) may assist your Company's efforts to operate and evaluate controls
- Both SAP Process Control and Oversight Systems function to provide assistance to management in monitoring the Company's controls environment

*Note, for the purposes of today’s presentation we have restricted the content to these two tools. However, there are other tools in the marketplace that are able to perform some of the functions mentioned in this presentation.*
Introduction

Current state: Businesses are in a constant state of change.
Current state

Businesses are always changing as they are always finding better ways to do what they do.

• New risks are continuously introduced by way of:
  - Expansion into new locations
  - Mergers and acquisitions
  - New processes
  - New technologies

• Other risks can become irrelevant as technology, processes and business units are decommissioned, centralised or standardized.

This leads to a need to perform **process optimizations**.
Process optimization

Process optimization is the activity of revisiting current processes, controls, and risks to refine the activities and perform the process more effectively. It usually is done through the following actions:

- Identify and replace inefficient controls or activities
- Remove controls or activities that are not needed
- Tailor current controls or activities to better fit with the business process and technologies
- Identify unmitigated risks and implement controls or activities that mitigate those risks

 Reduce unneeded activities and identify unmitigated risks
Challenge

How to balance cost and flexibility?
Finding balance

Businesses struggle to balance cost and flexibility

When determining how to best mitigate risk, there is an inherent struggle with balancing business flexibility and minimizing the cost of supporting controls. Typically, there is a trade-off between:

- Preventive configurable controls (low cost to implement and operate) and
- Detective controls (allow business processes flexibly at a much higher cost).
Configurable Controls

• Configurable controls:
  - Are low cost to implement and operate,
  - Prevent 100 percent of problematic transactions by disallowing these transactions to process, and
  - Are **absolute**.

• Most business processes cannot process transactions in exactly the same way 100 percent of the time as there are always exceptions to the norm. For example:
  - Financial close,
  - Small business units, and
  - Newly acquired businesses.
Issues with configurable controls
Configurable controls cause issues due to their inflexibility.

‘Carve-outs’
Detective control(s) are put in place to mitigate risk where the configurable control cannot be applied. This is problematic as detective controls are:

• Manual in nature and periodically performed,
• The exception to the norm,
• Costly to operate, and
• Normally performed on a sample basis because of the volume of transactions.

Circumvention of current processes and control
Preventive controls can cause the business users to circumvent the controls by use of back doors (i.e., superuser access, batch input, manual postings, or nonroutine functionality).

Business choke
Preventive controls can also unnecessarily choke processes whereby the configuration in the system essentially restricts the businesses from performing their day-to-day duties or processing transactions timely.
Continuous monitoring can enable companies to increase breadth of risk coverage and maintain business flexibility while minimizing business efforts to operate and evaluate controls, removing the need to make this trade-off.
Continuous monitoring: Definitions
Continuous monitoring is the process or technology that is used to constantly review something against expected criteria.

Continuous monitoring involves:

- The set of the expected criteria
- An automation to review against that criteria to identify exceptions
- A notification method (in most cases workflow or email based)

Continuous Control Monitoring (CCM)

A technique that analyzes configuration, master data or transactions to identify exceptions that would indicate an issue with that control’s effectiveness.

Example: monitoring the release strategy configuration for alignment with the expected configuration.

Continuous Transaction Monitoring (CTM)

A technique that analyzes all transactions or other data to identify exceptions that would indicate an abnormal (out of policy) transaction.

Example: monitoring all purchase orders processed to identify duplicate purchase orders or purchase orders processed outside budget or approval limits.
Examples of Continuous Monitoring: Focusing on CCM and CTM

CCM

Automated controls
Exceptions relating to configuration settings or parameters in the ERP system
- An exception is reported if the tolerance amount for the three-way match control for accounts payable invoices is changed.
- An exception is reported if the credit authorization approval control is turned off.

A CCM strategy for configurable controls provides Management with a proactive mechanism to identify when key application control settings have been changed.

CTM

Master data
Exceptions relating to governance of master data in the ERP system
- An exception is reported if the general ledger field structures have been modified in the master table.
- An exception is reported if changes (including creation, modification and deletion) are made to critical attributes defined in vendor master data.
- An exception is reported if changes have been made to the general ledger account code options and/or account mapping for automatic system processing functions.

A CTM strategy for master file data provides Management with a proactive mechanism to verify that the integrity of the master file architecture and content is not compromised.

Transaction data
Exceptions relating to business transactions within the ERP system based on available transaction data
- An exception is reported if a purchase order is created on the same day that goods were received for a transaction.
- An exception is reported if a manual journal entry has unusual accounts and/or descriptors.
- An exception is reported if an employee receives more than one pay distribution in a pay period.

A CTM strategy for transaction data provides Management with a proactive mechanism to identify potential control exceptions and fraudulent activity.
Control types and control monitoring

Preventive
- Manual approvals
- Physical access
- Segregation of duties/sensitive access
- System calculations
- Workflow (SAP)-based approvals

Automated preventive
- SAP GRC suite
- Configuration

Real-time detective
- Workflow (Oversight)-based alerts

Detective
- Physical counts and checks
- Detective report reviews
- Spreadsheet reconciliations

Controls

SAP tool to enable
- SAP GRC suite
- SAP ABAP Reports
- SAP Business Intelligence Reports

Frequency

Per transaction
- Low: Timeliness: High
- High: Effort to operate: Low
- Sample: Percentage coverage: 100%

Per transaction
- Multiple times a day to daily

Transaction monitoring
- Weekly, monthly, quarterly, biannually, annually

Continuous Monitoring: Match Your Business Needs with the Right Technique
PwC

September 2012
Control quadrant: Cost vs. flexibility

*Optimal state: Real-time detective controls with automated preventive supporting controls used to reduce exceptions
SAP’s continuous monitoring tools

SAP Process Control (core competency CCM) and SAP’s endorsed business solution, Oversight Systems (core competency CTM)
SAP process control and oversight systems’ attributes

Process Control

**Main Purpose:** Manage control or a compliance framework and support the evaluation of that framework.

- More efficient management of multiple compliance frameworks
- Easy overview of the state of controls at any given point.
- Issues with controls can be flagged in an automated fashion or reported in automatically through surveys
- Policy management
- Ability to monitor changes to configurable controls

Oversight Systems

**Main Purpose:** Manage business or transaction exceptions and support the operation of controls and processes.

- Very complicated analytics can be performed over extremely large data sets
- Easy follow-up enabled by background data for exceptions displayed, email integration, automatic logging of all activities for the exception
- Data is stored in Oversight enabling efficient analysis with no load on production
- The ability to create granular, flexible rules and the ability to use statistics to enable trending
SAP process control and oversight systems

Preventive
- Manual approvals
- Physical access
  - Workflow (SAP)-based approvals

Automated preventive
- Segregation of duties/sensitive access
- System calculations
  - Workflow (SAP)-based approvals

Real-time detective
- Workflow (Oversight)-based alerts

Detective
- Physical counts and checks
- Detective report reviews
- Spreadsheet reconciliations

Controls

SAP tool to enable
- SAP GRC suite
- Configuration

SAP Process Control

Frequency
- Per transaction
  - Low: Timeliness
  - High: Effort to operate
  - Sample: Percentage coverage

Oversight
- Multiple times a day to daily

Transaction monitoring
- Weekly, monthly, quarterly, biannually, annually
- High: Frequency/timeliness
- Low: Effort to operate

Control monitoring
- Sample: Percentage coverage
**PC and oversight real world examples**

Exchange rates

**SAP Process Control**

**Rule 1:** All changes to the exchange rate table trigger an exception.

- All exchange rate changes are reviewed in PC after the change has processed in ECC.
- This could trigger numerous exceptions, need to filter for more critical rates.

**Rule 2:** If an exchange rate fluctuates beyond an expected tolerance, an exception is triggered.

- Exchange rate changes over expectation are reviewed in PC after the change has processed in ECC.
- Updates to the tolerance levels would be required over time.

**Oversight Systems**

**Integrity check 1:** Exchange rates are compared with an external source. Rates that do not generate an exception.

- All inaccurate exchange rates are identified and escalated for resolution.
- Exception only reporting.

**Integrity check 2:** Exceptions are generated for any change to an exchange rate over a set standard deviation.

- All abnormal exchange rate changes over the threshold are identified for review.
- Exception only reporting but may not catch as many exceptions as IC#1.
PC and oversight real world examples
Vendor master records

SAP Process Control

**Rule 1:** All changes to vendor master records trigger an exception.
- All vendor changes are reviewed in PC after the change has processed in ECC.
- This could trigger numerous exceptions, need to filter for more critical company codes or restrictions to key fields.

**Rule 2:** Monitor configuration of dual approval controls and key fields defined.
- This will monitor the configuration in ECC that enforces review and approval for the critical vendor master fields. If a change is made to this configuration, an exception is generated in PC.

Oversight Systems

**Integrity check 1:** Key vendor fields (e.g. banking information) which are changed and changed back are flagged as exception.
- All change-change backs to vendors are flagged for resolution.
- Exception-only focused reporting.
- Oversight keeps it’s own change history so can identify changes made through back-doors (e.g. DBA level).

**Integrity check 2:** All vendor master with similar names, address, bank information, etc. are flagged for review.
- All potential duplicates are flagged follow-up.
PC and oversight real world examples

Duplicate invoices

SAP Process Control

Rule 1: Monitor configuration of duplicate invoice indicators.

• This will monitor the configurations in ECC that enforce flagging duplicate invoices. If a change is made to this configuration, an exception is generated in PC.

• This is a monitoring technique of the supporting configuration; it does not identify actual duplicate invoices.

Rule 2: Monitor vendor master records created without the duplicate checkfield activated.

• All vendors created without the proper configuration will be flagged for review.

Oversight Systems

Integrity check 1: Invoices to the same or similar vendor, with the same amount, same amount with different currencies, similar invoice numbers, and other key attributes are flagged.

• All potential duplicate invoices are flagged for review.

• This integrity check flags the actual duplicate invoices in addition to false positives (i.e., invoices that look duplicated but are actually valid).

• Tuning of integrity checks is vital to ensure that false positives are reduced to the greatest extent possible to ensure the exceptions are manageable.
PC and oversight real world examples

Invoices over budget

SAP Process Control

**Rule 1:** Invoices that exceed the set tolerance limits for user groups are flagged for resolution.

- All invoices which are potential splits to avoid budget configuration are flagged for review.

**Rule 2:** Tolerance levels for invoices are configured to trigger workflow exceptions for invoices above budget limits.

- All invoices above budget limits are flagged for review.

Oversight Systems

**Integrity check 1:** Transactions that are likely splits can be identified and compared to the chart of authority to flag exceptions.

- All invoices which are potential splits to avoid budget configuration are flagged for review.

**Integrity check 2:** POs and invoices that are above the norm (by evaluating the standard deviation over the history of transactions) for the vendor, buyer, or other criteria are flagged for resolution.

- All invoices which are potentially erroneous (e.g. by typos etc.) are flagged for review.
Using SAP process controls supporting control operation

If you are using SAP Process Control to support the operation of controls (not limited to evaluation of effectiveness of controls), keep in mind:

• Exceptions generated by a PC configuration acting as a control would not constitute a ‘deficiency’.

• These exceptions are meant to be reviewed and resolved as part of the control’s operation.

• Must consider this throughout the design of the PC environment to ensure that exceptions generated do not translate to a control failure.
The continuous monitoring roadmap

Where do you start?
Choose what you wish to achieve first:

Lower the cost to operate controls vs. lower the cost to evaluate controls

Where to start

First determine what benefits you wish to realize first from the tool. Deciding this and articulating it up front enables you to:

• Select the appropriate tool that supports that most immediate initiative

• Clearly articulate to the project team and stakeholders what will be met in the current phase of the roadmap and what will be accomplished with later functionality

• Successfully meet the stakeholders’ objectives
The continuous monitoring considerations

**Driver: Lower cost to operate controls**
- Reduce business efforts to operate controls (useful for clients with many manual controls)
- Identify business exceptions and control breakdowns sooner
- Increase business flexibility through moving toward real-time detective controls
- Achieve more coverage of risk
- Remove obvious pain points
- Stop known problematic transactions

**Driver: Lower cost to evaluate controls**
- Lower the cost of compliance functions efforts
- Identify control breakdowns sooner
- Lower the cost of business self-assessment of controls
- Achieve better visibility of the compliance framework and the overall state of risk
- Organize risks and controls in a more meaningful fashion
- Policy management to support controls

Then document the controls in your Continuous Control Monitoring Solution

Then implement controls in your Continuous Transaction Monitoring Solution
For further information, please contact:

Jamie Levitt  
Manager  
(949) 462 – 4592  
jamie.levitt@us.pwc.com

Ronald Risinger  
Senior Associate  
(949) 437 – 4489  
ronald.j.risinger@us.pwc.com

Certain matters reviewed today may represent services that PwC may be prohibited from providing to our audit clients. In those instances, the information is being provided to inform you of options that you may consider as you assess your company's approach to Continuous Monitoring. Independence rules are complex and we recommend to discuss all services with you in advance within the context of the independence rules. The information contained in this document is provided 'as is', for general guidance on matters of interest only. PricewaterhouseCoopers is not herein engaged in rendering legal, accounting, tax, or other professional advice and services. Before making any decision or taking any action, you should consult a competent professional adviser.

© 2012 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the United States member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.