Reduce Audit Time Using Automation, By Example

Jay Gohil
Senior Manager
Today’s Session

Speaker Bio: Jay Gohil, Protiviti
Jay is a Senior Manager in the ERP Services practice in Atlanta. In the past seven years, Jay has focused on SAP Security, Segregation of Duties, and Governance, Risk, and Compliance Access Control (GRC-AC) projects.

Topic:
• Defining and leveraging continuous controls monitoring (CCM)
• Understand how to move from ad-hoc manual audit testing to a more streamlined and automated approach and using SAP Process Control to continuously monitor risk.
• This session uses an example situation to address:
  • Maturing from manual testing to a more automated approach
  • Reviewing current tools for automation
  • How to identify and exploit SAP’s Process Control 10 solution to streamline control testing
Agenda

I. Background on Continuous Auditing and Monitoring
II. Terminology
III. Current Tools & Market Convergence
IV. Maturing From Manual To Automated
V. Example Scenario
Continuous Auditing vs. Continuous Monitoring

Continuous Auditing

Any method used by *auditors* to perform audit-related activities on a more continuous or continual basis.

Continuous Monitoring

A process that *management* puts in place to ensure that its policies, procedures, and business processes are operating effectively.

Source: The Institute of Internal Auditor's Global Technology Audit Guide (GTAG), *Continuous Auditing: Implications for Assurance, Monitoring and Risk Assessment*:
The Inverse Relationship between Continuous Auditing and Continuous Monitoring

Higher level of monitoring of controls = Lower level of detailed testing of controls need

Lower level of monitoring of controls = Higher level of detailed testing of controls needed

Management Response

Comprehensive Monitoring of Internal Controls

Little Monitoring of Controls

Reduced Effort

Significant Effort/Greater Resources

Audit Effort
Benefits

- Increased testing coverage (100% of population)
- Improved timeliness of testing
- Greater visibility
- Independent testing
- Identification of trends
- Improved consistency
- More efficient allowing focus on overall process efficiency and effectiveness
- Cost-effective solution

The Auditing Profession is entering the Age of Continuous Auditing

- Annual Audits are being viewed as untimely and obsolete
- Internal Control issues are expected to be reported almost immediately
### Terminology!

- **CA** – continuous auditing
- **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
Continuous Auditing/Monitoring Tools in the Market
Leaders in CCM

Gartner Magic Quadrant for Continuous Controls Monitoring

Source: Gartner’s website at http://www.gartner.com/

Tool Convergence

The vendors and associated products used for Continuous Audit have drastically changed in the past couple of years including:

- **Vendor Consolidation** (e.g. Infor acquires Approva, IBM acquires OpenPages and Algorithmics, EMC-RSA acquires Archer, Thomson Reuters acquires Paisley)

- Divergence amongst competitors focusing on **audit management vs. audit automation**

- Product **increased interoperability** to allow for a more integrated GRC platform (e.g. SAP GRC 10.0, Oracle GRC)

- Industry specific solution content becoming more important (e.g. Oil & Gas, Banking, Dodd-Frank, etc.)
A technology solution to support the oversight and operation of enterprisewide risk management and compliance programs, with the overall objective being improvements in corporate governance....

- Gartner
eGRC Components

- Content Management
  - Managing documentation related to policies, risks, controls, testing, configuration.

- Workflow / Alerts
  - Automating controls surrounding approvals, tasks, and alerts

- Transactional Analysis / Monitoring
  - Monitoring controls on a configuration and transactional level to determine if controls are operating as designed.

- User Access Reporting / Monitoring
  - Segregation of Duties (SOD) / Sensitive Access

- Configuration Monitoring
  - Automated / System Controls

- Dashboarding
  - Providing management with a comprehensive overview of the control / risk environment.
The Controls Challenge

Are we making unnecessary or unapproved discounts?

Have any POs been changed after approval?

Are people making unauthorized or incorrect manual entries to the GL?

Are purchasing cardholders violating company policy?

Am I losing money because of fraud?

Is anyone manually clearing blocked invoices?

Are we making duplicate payments?

Are my POs missing based on accurate vendor master data?

Are we at risk of an audit finding for user access?

Are we misclassifying assets as expenses?

Can users access sensitive information?

Are system configuration changes exposing me to risk?

Are we making duplicate payments?

Are we at risk of an audit finding for user access?

Are we misclassifying assets as expenses?

Can users access sensitive information?

Are system configuration changes exposing me to risk?
Trends and Leaders in eGRC

Gartner Magic Quadrant for eGRC

July 2011

challengers

leaders

Archer (EMC-RSA)
Enablon

B Wise
OpenPages (IBM)
Thomson Reuters
Oracle
MetricStream
SAP

LogicManager
SAS

BPS Resolver

Cura Technologies (Jade)
Active Risk

Achiever (Sword Group)

nich players

visionaries

ability to execute

completeness of vision

As of July 2011

October 2012

challengers

leaders

Thomson Reuters
IBM
EMC-RSA
Nasdaq-BWise
MetricStream

Protiviti

SAI Global Compliance

SA
Oracle
Software AG
SAS

Mega

Enablon

CMO Compliance
Jade Software-Methodware
BPS Resolver
Cura Technologies

nich players

visionaries

ability to execute

completeness of vision

As of October 2012

Source: Gartner’s website at http://www.gartner.com/
Business Controls – Where do you want to be?

Identification of Business Risks:
- Limited understanding of risks within each business process.
- Failure to classify the importance of business process risks

Configurable Controls:
- System application controls have not been documented or tested for effectiveness.
- Reliance is placed of manual process controls rather than taking advantage of system controls

Detective / Manual Controls / Business Rules / Policies:
- Controls are operating within the business but have not widely understood or formally documented.
- There is no link between key process risks and control items

Data Governance:
- Inconsistent and independent management of master data (vendor, customer, COA)

Continuous Control Monitoring:
- Regular testing and monitoring of both system and manual controls is not performed.
Maturing from Manual to Automated

Continuum

- **Optimized**
- **Managed**
- **Defined**
- **Repeatable**
- **Initial / Adhoc**

**Fully Automated**: Use of sophisticated tools to automate testing and aligning with business controls. Exceptions are reportable and monitoring is implemented for transactions and configurations.

**Semi-Automated**: Automation is used to perform testing across full populations. Use of tools (ACL or databases) to reduce analysis time.

**Manual**: Pull data at the time of testing and performing sample based testing.
Example Scenario:
One Time Use Vendors
Scenario

• Creation of vendors is tightly controlled
• Often times, it’s necessary to bypass system checks to create “one-time vendors”
• Used on an exception basis, allowing user to bypass controls and push purchases through

• **Control Objective**: Purchases against one-time use vendors cannot exceed $10,000

• **Business Rule**: The sum of invoices to one-time use vendors should be less than $10,000
Example: Semi-Automated Control Test

- **Step 1:** Identifying the data
  - Select field → Help (F1) → Technical Information (Hammer/Wrench icon)
Example: Semi-Automated Control Test

Step 2: Obtaining the data based on frequency
- Method 1: Pull the data manually during each audit
- Method 2: Reliance on IT to provide the data – PARTNER!
  - Pulling data files from a staging location / folder
- Validate the accuracy and completeness of the data

Step 3: Automate the test using Excel / ACL / Access
- Requires detailed documentation of data requirements and scripts
- Skill-set with tools is sometimes lost with team member rotation

<table>
<thead>
<tr>
<th>Application</th>
<th>Ease of Use</th>
<th>Cost</th>
<th>Repeatability</th>
<th>Assurance of Data Integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excel</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Access</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>ACL</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>
Identifying the Data Source: SAP Structures

Identify transparent tables related to a structure:

- Right-click on a field containing data and click “Help (F1)"
- Click the "Technical Info" icon (hammer and wrench).
- Make a note of the table name and table category (e.g., Struct.) located in the Field Data section of the Technical Information window.
  - For the purpose of this example, let's assume the category is "Struct."
- In SAP, Execute T-Code SE84 (ABAP Workbench) and browse to ABAP Dictionary > Structures.
- Enter the structure name and click the Execute button (look for the green checkmark).
- Click the "Complete List" button to view additional fields.
- Make a note of the "Package" name.
- Browse to ABAP Dictionary > Database Tables (in SE84).
- Enter the Package name and click Execute
- Review the SAP tables related to the data element

Reference: Posted on LinkedIn Atlanta ACL User Group by John Buchanan on 8/15/2013
Example: Continuous Monitoring Using SAP Process Controls 10.0
CCM – Bigger Picture

Define Data Source and Business Rules
- Delivered rules, queries and reports
- Configurable rules
- Custom Programs

Map to Controls
- Transaction Controls
  - FIN
  - O2C
- Master Data Controls
  - P2P
  - HR
- Configuration Controls
  - IT
  - Fixed Assets

Test or Monitor

Analyze and Remediate
- Auditability
- Xcelsius Dashboards and Analytics
- Root cause analysis
- Crystal Reports
- Workflows

Report
Data Sources

- Subsets of data associated with business rules or controls
- Predefined queries for specific data elements
- The job of a data source (in GRC) is to provide a business-user-friendly view of technical data

SAP Process Controls 10.0

- **Note**: Data sources can and should be used for multiple rules or controls
  - May require bigger picture thinking and design discussions
Data Sources (continued)

- Intellectual property for table and field names
- User friendly interface to the data
Identify and Define Business Rules/Controls
Business Rules

- User specified logic based on business controls
- Business rules filter the data stream coming from data sources
- These rules can also perform calculations on the data
- Rules define exception situations
- Examples:
  - Total spend on a one-time vendor should not exceed $10,000

Rule Types
- Transactional (CCM-T)
- Configuration (CCM-AC)
Rule Type: Configuration Monitoring

- Rules based on the entries of log files
- Prerequisite: logging must be enabled on specific tables or specific areas
- Non-transactional patterns, such as flags or toggles
- Ability to run monitoring rule against an entire timeframe and reconstruct settings to identify changes that violate the rule
- Example:
  - Master data changes - enable/disable vendor blocked for credit status
  - Configuration changes

“My audit test is a point in time so how do I know that the configuration wasn’t changed for a short period of time and then changed back?”
Change Log Example

- **Control Objective**: Customer credit checks are performed based on category of customer, company code, and sales area for high risk sales orders.
# CCM – Sample Exception Report

## General Data
- **Test Result:** Fail
- **Test Date:** 07.03.2012
- **Scheduled By:** VJPAT01
- **Test Automation:** Automated

## Rules
<table>
<thead>
<tr>
<th>Results</th>
<th>Business Rule</th>
<th>Exceptions</th>
<th>Deficiency Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail</td>
<td>PDS - FC - Journals to Rec Accts</td>
<td>97</td>
<td>High</td>
</tr>
<tr>
<td>Fail</td>
<td>PDS - FC - Journals Unapproved Users</td>
<td>155</td>
<td>High</td>
</tr>
<tr>
<td>Fail</td>
<td>PDS - FC - Journals Over Amount</td>
<td>24</td>
<td>High</td>
</tr>
</tbody>
</table>

## Details

<table>
<thead>
<tr>
<th>Sequence Number</th>
<th>Deficiency Type</th>
<th>Deficiency Description</th>
<th>Company Code</th>
<th>Accounting Document Number</th>
<th>General Ledger Account</th>
<th>Debit/Credit Indicator</th>
<th>User Name</th>
<th>Amount in Local Currency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>High</td>
<td>Direct journals over $10 million</td>
<td>1000</td>
<td>0100000353</td>
<td>0000085900</td>
<td>H</td>
<td>OTTENBACHER</td>
<td>13.889.960,50</td>
</tr>
<tr>
<td>2</td>
<td>High</td>
<td>Direct journals over $10 million</td>
<td>1000</td>
<td>0100000354</td>
<td>0000085900</td>
<td>S</td>
<td>OTTENBACHER</td>
<td>13.889.960,50</td>
</tr>
<tr>
<td>3</td>
<td>High</td>
<td>Direct journals over $10 million</td>
<td>1000</td>
<td>0100000355</td>
<td>0000085900</td>
<td>H</td>
<td>OTTENBACHER</td>
<td>13.889.960,50</td>
</tr>
<tr>
<td>4</td>
<td>High</td>
<td>Direct journals over $10 million</td>
<td>1000</td>
<td>0100000356</td>
<td>0000085900</td>
<td>S</td>
<td>OTTENBACHER</td>
<td>13.889.960,50</td>
</tr>
<tr>
<td>5</td>
<td>High</td>
<td>Direct journals over $10 million</td>
<td>1000</td>
<td>0100007875</td>
<td>0000113101</td>
<td>S</td>
<td>OTTENBACHER</td>
<td>86.840.605,34</td>
</tr>
<tr>
<td>6</td>
<td>High</td>
<td>Direct journals over $10 million</td>
<td>1000</td>
<td>0100007877</td>
<td>0000113101</td>
<td>H</td>
<td>D023346</td>
<td>86.840.605,34</td>
</tr>
<tr>
<td>7</td>
<td>Medium</td>
<td>Direct journals over $1 million</td>
<td>1000</td>
<td>0100004038</td>
<td>0000113102</td>
<td>S</td>
<td>FREUNDEK</td>
<td>1.017.034,72</td>
</tr>
<tr>
<td>8</td>
<td>Medium</td>
<td>Direct journals over $1 million</td>
<td>1000</td>
<td>0100004041</td>
<td>0000113102</td>
<td>S</td>
<td>FREUNDEK</td>
<td>7.240.202,68</td>
</tr>
<tr>
<td>9</td>
<td>Medium</td>
<td>Direct journals over $1 million</td>
<td>1000</td>
<td>0100004074</td>
<td>0000113109</td>
<td>H</td>
<td>FREUNDEK</td>
<td>2.809.241,85</td>
</tr>
<tr>
<td>10</td>
<td>Medium</td>
<td>Direct journals over $1 million</td>
<td>1000</td>
<td>0100004078</td>
<td>0000113109</td>
<td>H</td>
<td>FREUNDEK</td>
<td>1.350.326,37</td>
</tr>
<tr>
<td>11</td>
<td>Medium</td>
<td>Direct journals over $1 million</td>
<td>1000</td>
<td>0100004079</td>
<td>0000113109</td>
<td>H</td>
<td>FREUNDEK</td>
<td>1.698.743,62</td>
</tr>
</tbody>
</table>
A Few Key Points to Take Home

To achieve your continuous compliance objectives:

• Identify your compliance needs and the risks to address them
• Understand the controls in place to mitigate the risk
• Identify the data sources and partner with IT to obtain accurate and complete data
• Convert your controls into business rules for automation
• A continuous risk and controls assurance program is enabled by technology
Complimentary SAP Process Control Webinar

http://www.protiviti.com/webinars
Look for the event: *Identifying the Value SAP Process Control Can Deliver to Your Organization*
Thank You

Jay Gohil
Jay.Gohil@protiviti.com
LinkedIn.com/in/JayGohil

Powerful Insights. Proven Delivery.™