A Case Study in Continuous Controls Monitoring

Presented to:

GEEK WEEK
ISACA Atlanta

August 20, 2013
Course goals & objectives

- To guide participants through the terminology, concepts and value proposition for deploying Continuous Controls Monitoring (CCM).
  - Review of what CCM is
  - Benefits of CCM
  - Required Components
  - Discuss the Emory Case Study
  - Tools to leverage
  - The Approach and Best Practices
  - Discuss Emory’s ROI
About the Presenters

- **Mark Hafitz – Director of Information Technology Special Projects**
  As well as being an Emory alumnus, Mark has worked for Emory University for over 20 years. His career at Emory started in the Information Technology Division working as a Programmer/Analyst supporting financial applications. Several years later he began working in the Human Resources Division as the Assistant Director, Information Systems. He managed the daily operations of the Human Resources Information Systems area and oversaw the development and maintenance of all Human Resources systems. For the last 15 years he has worked in the Finance Division managing and overseeing the completion of the division wide financial systems projects as the Director of Financial Projects. Prior to Emory, Mark spent several years as a Programmer/Analyst working with the Information Systems group at Kimberly-Clark Corporation. Mark received his Master of Business Information Systems degree from Georgia State University, and a Bachelor of Arts in English Literature from Emory University.

- **Michael Lisenby, Managing Partner Solomon Edwards- Atlanta**
  Mike Lisenby is a specialist in Enterprise Risk Services & Compliance. Mike has over 16 years of experience in helping businesses manage their accounting, finance, technology resources and compliance needs effectively. Mike’s experience includes consulting and co-sourcing, IT audits, SOX compliance, and technology security assessments, risk identification, assessment and evaluation; risk response; risk monitoring; IT control design and implementation; and IT control monitoring and maintenance. Mike held leadership roles with Arthur Andersen and several other National Consulting Firms, and has prior internal audit experience with Fortune Brands and Philip Morris. He currently holds a CRISC (Certified in Risk and Information Systems Control) Certification.
What is CCM

- Continuous Controls Monitoring (CCM) is an ongoing systematic practice of observing and checking, for reasonable assurance, that Information Technology Systems (hardware and/or software) operate as designed. These supervisory practices, against IT systems, have a basis for maintaining data validity, reliability, and integrity. Several areas where modern organizations depend on IT systems to operate continuously, accurately and effectively:
  - The reporting of organization finances.
  - E-Commerce and Electronic Funds Transfer.
  - Medical, Criminal, or Federal Data Records Management and Retention.
  - Public Telecommunications Voice and Data Networks
  - National Energy Grids and Utilities.

-Wikipedia
Benefits of CCM

- Process problems are reflected in transactional data if you know what to look for.
- 100% of transactions tested with sophisticated analytics in near real-time (as opposed to a periodic sample long after occurrence).
- Results can be acted on rapidly, sometimes before transaction cycle completes.
- Goes beyond just “reporting” to provide an actionable control framework.
- Cutting costs, catching policy violations or fraud – Ex: T&E expense submissions.
- Automate manual tasks – Ex: Reconciliations, IA testing procedures, access controls.
- Stopping Revenue Leakage – Ex: sales or source documents that trigger revenue recognition missing.
Components of CCM

Source Systems

- GL
- AP
- AR
- HR
- Other

Replication or ETL

Replicated Data for Analysis

Statistical and Analytical Routines Continuously Performed on Data

Reports & Dashboards

Exception Management Interface

Email Alerts

Exceptions Identified

Invoice A123 from “Acme Solutions” in the amount of $543.21 may be a duplicate of invoice 123-1 in the amount of $543.21 Dated 4-14-2010 from “Acme Inc.”
Approach

Step 1: Design Controls
- Workshop(s):
  - Determine Risks and Control Use Cases needed
  - Understand the systems involved
  - Understand the Data
  - Define Analytical Logic needed, by Use Case
  - Define Exception Resolution workflow & Status Codes
  - Develop High Level Architecture
  - Security Requirements

- Create Design Document

Step 2: Implement ETL
- Collaborate w/ IT:
  - Set up hardware & Connectivity
  - Select ETL Approach
  - Develop ETL process
  - Develop Transformations, if required
  - Test Integrity and Impact on Production Environment
  - Start scheduler/Cron job

- Analytics DB In Place
- Create Exceptions DB

Step 3: Develop Analytics
- Iteratively for Each Use Case:
  - Develop Algorithm(s)
  - Unit Testing: Review and refine to reduce false positives
  - Set up Reports & Dashboards Tool (IIS or SharePoint)
  - Set up Exceptions Management Interface
  - System Documentation

Step 4: User Components
- Develop Reports & Dashboards
  - User Training
  - User Acceptance Testing
  - Tuning & Optimization

- Develop Email Alerts (Optional)
- Roll Out
Step 2: Implement ETL

Export Transform & Load

- Multiple ways to approach:
  - Linked Server Object (typical for an Oracle DB Source)
  - ETL Tools (such as SSIS; open source tools are available too)
  - Replication (Publication/Subscription model)

- If Mirror or Replicated instance of production data is already available that is the preferred method. If not, indexed short running queries with “Read Only” accounts to pull in daily incremental activity and only from needed tables/columns, based on scheduled job (during non-peak hours) is recommended.

- Key objective is automated availability of near real-time data needed to support continuous analytics

- Example of possible “Transformation”: Mapping might be needed to translate to parent’s Chart of Accounts or other common model from various autonomous systems to allow cross-comparisons

- Some analytics need to track “changes” to Master Data (Example: Vendor Master File Tampering Testing); in this case, we created logic to create versioned snapshots of records in the ETL logic

- Because we want the Exception to be able to be resolved by the Owner without them having to log into the source application, we pull all data needed to understand and resolve the Exceptions for presentation in the Exception Report
## Specific Indicators

<table>
<thead>
<tr>
<th>Name</th>
<th>Duplicate Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Test for multiple occurrences of the same Amount being referenced by multiple invoices from the Same Vendor.</td>
</tr>
<tr>
<td>Functional Logic / Algorithm</td>
<td>For each given voucher, test all vouchers within the previous 60 days from the same vendor that are for the same amount.</td>
</tr>
<tr>
<td>Probability</td>
<td>20%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Duplicate PO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Test for multiple occurrences of the same PO number being referenced by multiple invoices.</td>
</tr>
<tr>
<td>Functional Logic / Algorithm</td>
<td>For each given voucher, test all vouchers within the previous 60 days for the same PO number being referenced.</td>
</tr>
<tr>
<td>Probability</td>
<td>80%</td>
</tr>
</tbody>
</table>

Each Indicator becomes a part of the Where Clause and possibly helps drive joins.
Multiple Indicators in SQL

Select
Exception ID (key),
‘Duplicate Invoice’ as ‘Exception_Type’,
XXX as Probability,
Etc... (All data needed)

From Vouchers as V

Join Vouchers as V_Same_PO
    on V.PO = V_Same_PO.PO

Join Vouchers as V_Same_Amt
    on V.Amt = V_Same_Amt.Amt

Where V.Vendor + V.InvNo <>
    V_Same_PO.Vendor + V_Same_PO.InvNo

And (V_Same_PO.VoucherNum not Null
    OR
    V_Same_Amt.VoucherNum not Null)
The “Probability” field in your select clause:

Select
'Probability' =
(case WHEN V.PO = V_Same_PO.PO THEN 80% end) + (case when V.Amt = V_Same_Amt.Amt then 20% end)
From Table_X
Duplicate Invoice Actual Script

--5.7B Possible Duplicate Invoice: Same Invoice No and Amount for Similar Vendors, within 60 days.
Insert into CCM.dbo.EXCEPTIONS_Stage
SELECT
Case when V_Dup.BUSINESS_UNIT in ('EMUNV') then 'EUV' else 'EHC' end AS COMPANY,
null AS DEPT_NUM,
null AS DEPT_NAME,
EXCEPTION AS TYPE,
'Procure to Pay' AS CATEGORY,
'
EXCEPTIONID,
GETDATE() AS EXCEPTION_DATE,
V_Dup.OPRID_LAST_UPDT AS ASSOCIATED_USER, 'NEW' AS STATUS,
null AS EXCEPTION_OWNER,
null AS NOTES,
INDICATORS = (case when CCM.dbo.fn_StrClean(ISNULL(V_Prior_Addr.ADDRESS1, ' ')) + ISNULL(V_Prior_Addr.ADDRESS2, ' ') + ISNULL(V_Prior_Addr.City, ' ') = CCM.dbo.fn_StrClean(ISNULL(V_Dup_Addr.ADDRESS1, ' ') + ISNULL(V_Dup_Addr.ADDRESS2, ' ') + ISNULL(V_Dup_Addr.City, ' '))
then 'Same Invoice Number for Vendors with Similar Address.'
else '
end) +
(Case when CCM.dbo.fn_calculateJaroWinkler(CCM.dbo.fn_StrClean(ISNULL(V_Name_Dup.NAME1, ' ')), CCM.dbo.fn_StrClean(ISNULL(V_Name_Prior.NAME1, ' '))) > .97
then .6
else (.5-.5)
End),
V_Dup.GROSS_AMT AS FINANCIAL_IMPACT,
VAL_1 = V_Dup.INVOICE_ID,
DEF_1 = 'Duplicate Invoice No.',
VAL_2 = V_Prior.INVOICE_ID,
DEF_2 = 'Prior Invoice No',
VAL_3 = V_Dup.GROSS_AMT,
DEF_3 = 'Invoice Amt',
VAL_4 = V_Dup.Voucher_ID,
DEF_4 = 'Duplicate VoucherID',
VAL_5 = V_Prior.Voucher_ID,
DEF_5 = 'Prior Voucher ID',
VAL_6 = V_Dup.VENDOR_ID,
DEF_6 = 'Duplicate Vendor ID',
VAL_7 = V_Prior.Vendor_ID,
DEF_7 = 'Prior Vendor ID',
PR

Step 3: Develop Analytics

Script Development (continued)
Duplicate Invoice Actual Script (Continued)

VAL_8 = V_Name_Dup.NAME1,
DEF_8 = 'Duplicate Vendor Name',
VAL_9 = V_Name_Prior.NAME1,
DEF_9 = 'Prior Vendor Name',
VAL_10 = V_Dup.Invoice_DT,
DEF_10 = 'Duplicate Invoice Date',
VAL_11 = V_Prior.INVOICE_DT,
DEF_11 = 'Prior Invoice Date',
VAL_12 = CCM.dbo.fn_StrClean(ISNULL(V_Dup_Addr.ADDRESS1, ''
+ ISNULL(V_Dup_Addr.ADDRESS2, '') +
ISNULL(V_Dup_Addr.City, '')
),
DEF_12 = 'Scrubbed Duplicate Vendor Address',
--VAL_13 =
CCM.dbo.fn_StrClean(ISNULL(V_Prior_Addr.ADDRESS1, '') +
ISNULL(V_Prior_Addr.ADDRESS2, '') +
ISNULL(V_Prior_Addr.City, '')
),
DEF_13 = 'Scrubbed Prior Vendor Address',
VAL_14 = NULL,
DEF_14 = NULL,
VAL_15 = NULL,
DEF_15 = NULL,
VAL_16 = NULL,
DEF_16 = NULL,
VAL_17 = NULL,
DEF_17 = NULL,

from CCM.dbo.PS_VOUCHER as V_Dup
left outer join CCM.dbo.PS_VOUCHER as V_Prior
on V_Prior.INVOICE_ID = V_Dup.INVOICE_ID
and V_Prior.VENDOR_ID != V_Dup.VENDOR_ID
and V_Prior.INVOICE_DT >= DATEADD(dd, -60, V_Dup.INVOICE_DT)
and V_Dup.ENTERED_DT >= V_Prior.ENTERED_DT
left outer join CCM.dbo.PS_VENDOR as V_Name_Dup
on V_Name_Dup.VENDOR_ID = V_Dup.VENDOR_ID
left outer join CCM.dbo.PS_VENDOR as V_Name_Prior
on V_Name_Prior.VENDOR_ID = V_Prior.VENDOR_ID
left outer join CCM.dbo.PS_VENDOR_ADDR as V_Dup_Addr
on V_Dup_Addr.VENDOR_ID = V_Dup.Vendor_ID
and V_Dup_Addr.ADDRESS_SEQ_NUM = V_Dup.ADDRESS_SEQ_NUM
left outer join CCM.dbo.PS_VENDOR_ADDR as V_Prior_Addr
on V_Prior_Addr.VENDOR_ID = V_Prior.Vendor_ID
and V_Prior_Addr.ADDRESS_SEQ_NUM = V_Prior.ADDRESS_SEQ_NUM
where V_Dup.ENTERED_DT >= DATEADD(dd, -5, V_Dup.INVOICE_DT)
and V_Prior.ENTRY_STATUS NOT IN ('X', 'R')
and V_Prior.Vendor_ID is not null
and V_Dup.GROSS_AMT = V_Prior.GROSS_AMT
and ( CCMDdbo.fn_StrClean(ISNULL(V_Prior_Addr.ADDRESS1, '') +
ISNULL(V_Prior_Addr.ADDRESS2, '') + ISNULL(V_Prior_Addr.City, '')
) = CCM.dbo.fn_StrClean(ISNULL(V_Dup_Addr.ADDRESS1, '') +
ISNULL(V_Dup_Addr.ADDRESS2, '') + ISNULL(V_Dup_Addr.City, '')
) OR

CCM.dbo.fn_calculateJaroWinkler(CCM.dbo.fn_StrClean(ISNULL(V_Name
_Dup.NAME1, ''
),
CCM.dbo.fn_StrClean(ISNULL(V_Name_Prior.NAME1, ''
) > .97
);
Case Study – Issues

- Significant Control Weaknesses
  - Decentralized structure
  - Multiple disbursement processes
  - Broadly distributed access
  - Duties not segregated
  - Few restrictions/discretionary accounts
  - Poor monitoring controls

- Bleeding From a Thousand Cuts
  - 1 million annually in inaccurate payments
  - Multiple frauds

- Resource Limitations
Case Study – Considerations

- Desire to be “Proactive vs. Reactive”
  - Catch errors before paid

- Budget
  - No Licensing fees/annual commitments

- Flexibility/Ease of Use
  - Audit department to maintain/minimal IT support
  - Growth potential: handle unlimited data sources and continually add new logic tests
  - Communications (notice of exceptions; resolution)
  - Transferability to management
  - Reporting capabilities

- Security & Compliance
  - The environment needed to be secure (SSL) to safeguard confidential information
Case Study – Why SEG

- Why Emory decided to Partner with SEG and use an open-source solution:
  - Subject Matter Expertise
  - Cost effective/No additional licensing fees
  - Co-Sourced Approach
  - Leveraged use of existing technology/Not tied to vendor
  - Knowledge transfer/ability to support in house
  - Ability to deploy in a phased approach
Algorithms Created – Phase I

- Vendor Master Integrity Checks
  - Conflicts of interest
  - Duplicate vendors
  - Vendor Master Tampering

- Payment Integrity Checks
  - Duplicate Payments
  - Potential personal purchases on corporate card
  - Expenses/ Per Diems
  - Travel agent/employee ID not validated

- HR Checks
  - Rehire of terminated employees
  - New hire background checks
  - FMLA Status Consistency
  - FLSA Error Checking
Components of CCM At Emory

Source Systems

- PeopleSoft
  - HR,
  - Payroll,
  - Payables,
  - Procurement
- Kronos
- LDAP
- VB Script

SQL Replicated Data For Analysis

Statistical and Analytical Routines Continuously Performed on Data

Exceptions Identified

Email Alerts generated embedded link to a report

Reporting Tool

IIS Web Based Reports & Dashboards

Exception Management Interface

ASP.net Web form

Email Alerts

Generated embedded link to a report
Automated Processing

- Automated notification of daily ETL feed and Analytics Success for Failure is sent to management, giving positive assurance that the application is continuously testing transactional data. Most days, no exception occurs, and there is nothing to report, so this allows confidence that the application is actually turned on and working.
Email Alerts

- When exceptions do occur, user specific Email Alerts are generated (when exceptions relevant to only specified users occur) with an embedded link to a report that only allows them to see authorized data unique to that user.
SSL Encryption

The SSL features in IIS cannot be used until you obtain and assign a server certificate to the computer that is running IIS.

Configuring SSL encryption is a multistep process that involves the following:
1. Requesting a server certificate for the computer that is running IIS. If the IIS server already has a server certificate, you can go to step 4.
2. Obtaining a server certificate from a certification authority.
3. Installing the newly issued server certificate into IIS, Binding it.
4. Enabling SSL encryption.
5. Updating the database of trusted Certification Authority on each smart device so it can recognize the server certificate as authentic.
Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

<table>
<thead>
<tr>
<th>Name</th>
<th>Issued To</th>
<th>Issued By</th>
</tr>
</thead>
<tbody>
<tr>
<td>WMSvc-AXEISE3LH</td>
<td>WMSsvc-AXEISE3LH</td>
<td>WMSsvc-AXEISE3LH</td>
</tr>
</tbody>
</table>

Actions:
- Import...
- Create Certificate Request...
- Complete Certificate Request...
- Create Domain Certificate...
- Create Self-Signed Certificate...

Help
Binding Certificate
Verify Binding
Configure SSL Settings

This page lets you modify the SSL settings for the content of a Web site or application.

- Require SSL
- Require 128-bit SSL

Client certificates:
- Ignore
- Accept
- Require

Actions:
- Apply
- Cancel
- Help
  - Online Help
# IIS Reporting

## Payroll Exception Report

<table>
<thead>
<tr>
<th>Exception Name</th>
<th>DEPT NUM</th>
<th>DEPT NAME</th>
<th>EXCEPTION ID</th>
<th>EXCEPTION OWNER</th>
<th>NOTES</th>
<th>EXCEPTION DATE</th>
<th>ASSOCIATE D USER</th>
<th>STATUS</th>
<th>INDICATOR S</th>
<th>PROBABILITY</th>
<th>FINANCIAL IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicate Tuition or Scholarship Payment</td>
<td></td>
<td></td>
<td>Total Number of Exceptions:</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S2A Multiple Jobs With F&amp;A Inconsistencies</td>
<td></td>
<td></td>
<td>Total Number of Exceptions:</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**View Report**
## IIS Reporting

![Image of an IIS Reporting interface showing data on exceptions and payroll records.](image)

### Exception Details:

<table>
<thead>
<tr>
<th>Exception Name</th>
<th>DEPT NUM</th>
<th>DEPT NAME</th>
<th>EXCEPTION ID</th>
<th>EXCEPTION OWNER</th>
<th>NOTES</th>
<th>EXCEPTION DATE</th>
<th>ASSOCIATED USER</th>
<th>STATUS</th>
<th>INDICATOR</th>
<th>PROBABILITY</th>
<th>FINANCIAL IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicate Tuition or Scholarship Payment</td>
<td>5361000</td>
<td>WWG Nursing Administration</td>
<td>5361000727490</td>
<td>07/08/11</td>
<td>12:09:00 AM</td>
<td>Mbis</td>
<td>NEW</td>
<td>Active Employee on FMLA Leave with concurrent active job record showing non FMLA Status</td>
<td>1.00</td>
<td>1.0000</td>
<td></td>
</tr>
</tbody>
</table>

---

**PAYROLL**

![Image of a payroll interface showing details of payroll entries.](image)
Clicking the above link presents an Alternate view of all data related to that specific exception.
Scrolling down to bottom, the user can click the link to enter “Edit Mode” (shown on next screen shot).
Edit Mode
Edit Mode

- After updating the information, user clicks the “Update” link
## Management Reporting

### Exception Table

<table>
<thead>
<tr>
<th>Exception Name</th>
<th>DEPT NUM</th>
<th>DEPT NAME</th>
<th>EXCEPTION ID</th>
<th>NOTES</th>
<th>EXCEPTION DATE</th>
<th>ASSOCIATE D USER</th>
<th>STATUS</th>
<th>INDICATOR S</th>
<th>PROBABILITY</th>
<th>FINANCIAL IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicate Tuition or Courtyard Scholarship Payment</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple Jobs With FMLA Ineligibilities</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WWJAH Nursing Administration</td>
<td>338000</td>
<td>WWJAH Nursing Administration</td>
<td>1234567890</td>
<td></td>
<td>3/9/2013 12:00 AM</td>
<td>1234567890</td>
<td>NEW</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Exceptions

- 5.17
  - Total Number of Exceptions: 5
  - Exception ID: 5
  - Notes: None
  - Exception Date: NA
  - Associate D User: NA
  - Status: NA
  - Indicator S: NA
  - Probability: NA
  - Financial Impact: NA

- 5.24
  - Total Number of Exceptions: 1
  - Exception ID: 1
  - Notes: None
  - Exception Date: NA
  - Associate D User: NA
  - Status: NA
  - Indicator S: NA
  - Probability: NA
  - Financial Impact: NA

- 338000
  - Exception ID: 338000
  - Notes: Active Employee on FMLA Leave with concurrent active job not showing non FMLA Status
  - Exception Date: 3/9/2013 12:00 AM
  - Associate D User: 1234567890
  - Status: NEW
  - Indicator S: 1.00
  - Probability: 1.0000
  - Financial Impact: 1.0000
  - Employee Name: Morgan Myfan

---

[Image of a software interface showing exception details and filtering options]
Case Study - ROI

- Implementation costs recovered in 6 weeks
  - Duplicate payments (invoices and supplemental pay)
  - Caught prior to disbursement (reduced costs to correct)

- Control Effectiveness Monitoring Results
  - Conflicts of interest
  - Expenses/ Per Diems
  - Rehire of terminated employees
  - Inconsistent FMLA status
  - Travel agent/employee ID not validated

- Future Opportunities/Next Steps
  - Revenue
  - RAC Audits
  - Compliance: grants and contracts
  - Removal of network access for terminated employees
  - Statistical analysis
Case Study - Results

Duplicate Payments: April 1 - July 31

Number of Exceptions - All Tests
Does CCM Make Sense For Your Company?

- Any manual processes subject to human error?
- Any Manual Audits or Reconciliations?
- Any recurring Analytical procedures that consume a lot of time or are pain-points?
- Concerns about policy compliance?
- Concerns about employee theft?

*If the answer is “yes” to any of these, it is likely that CCM can bring solid value to your company enabling you to increase its Audit Capability Maturity Level while allowing the finance and audit teams to show their strategic value to the rest of the company.*
For More Information

Mike Lisenby, CRISC
SolomonEdwards
Managing Partner
mlisenby@solomonedwards.com
Office: 404-497-4152
Mobile: 404-281-8005

Scott Stevenson, CIA, CPA
Emory University
Associate Chief Audit Officer
Office: 404-686-2916
sjsteve@emory.edu

SolomonEdwardsGroup, LLC
Atlanta Office
Five Concourse Parkway, Suite 1450
Atlanta, Georgia 30328