Successful Implementation of Continuous Controls Monitoring

Mady Cheng, CIA, CISA, CPA, MSBA
Franco Lopez, CIA, CISA, CPA, MBA
Office of Audits & Advisory Services • County of San Diego

March 12, 2014
Needle in a Haystack?

Found It!!!

Congratulations, it only took you 65298 seconds
Agenda

- Building Blocks

- Process
  - Conceptual Design
  - Project Implementation
  - Deployment

- Lessons Learned
Continuous Controls Monitoring Program

Building Blocks

Approach

Structure

Data

People

Communicate
Approach

• Focus on **high-impact analytics**. Less is more.
• Rank potential analytics based on risk and impact.
• Solicit input from business process Subject Matter Experts.
Data

- Understand your data (where it comes from, what it means, how it is used in the analytic). Work with DBA. Get data dictionary.
- Direct Access vs. Extracts.
- Trust but verify. Test, test, test... User Acceptance Testing.
People

- Cast vision. Gain **Buy-in** from users. “What’s there for me?”
- Educate users on benefits and regulatory requirements.
- Set the stage... avoid the abusive use of the “F” word (**False Positive**).
- Make system user-friendly. Make users’ job easier, not more difficult.
- Provide training and user manual.
Communicate

- Communicate, Communicate, Communicate – More, Early.
- **Listen.** Address complaints and concerns honestly and proactively.
- **Audience-oriented Messages** – What they need to know, what they can understand. Internal (within the organization) vs. External. Management vs. Business Users vs. Technical IT Personnel.
Structure

• Identify key stakeholders. Establish a **Sustainable Structure**: Steering Committee, Advisory Board, QA, System Admin, Users.
• System ownership and independence. Monitoring vs. Auditing.
• Project team: ACL Consultants, IT, Business Process SME, Facilitator.
• Set *expectations*. Define *roles and responsibilities*. Develop *policies*. 
Agenda

- Building Blocks

- **Process**
  - Conceptual Design
  - Project Implementation
  - Deployment

- Lessons Learned
Conceptual Design =
Put your **Building Blocks** in action!
Current Modules
- P-Card
- Procure-to-Pay

Analytic Objectives
- Proper Segregation of Duties
- Proper Authority and Approval
- Preventing Duplicate Payments
- Flagging Suspicious Vendors and Transactions
- Flagging Potential Conflicts of Interest
A1. Invalid Cardholder
A2. Similar Cardholder Addresses
A3. Merchant Employee Match - Tax ID/SSN
A4. SOD – Inappropriate Cardholder Role
A5. SOD – Inappropriate Verifier Role
A6. SOD – Inappropriate Approver Role
A7. SOD – Approver same as Verifier/Cardholder
A9. Same Merchant Same Amount Different Departments
A10. Same Merchant Same Amount Same Department
A11. Similar Merchants Similar Amounts (P-Card vs. AP Invoice)
A12. Lost/Stolen/Suspended Card
A13. Disputed Transaction
A14. Restricted Word

Monitored by:
• Depts
• Purchasing
• A/P
Email Notifications

• **Day 11**: Email to *Monitor*

  ![AX](image1) ➔ Monitor

• **Day 21**: Email to *Monitor* and *Manager*

  ![AX](image2) ➔ Monitor Manager

• **Day 41**: Email to *Monitor*, *Manager*, & *Internal Audit*

  ![AX](image3) ➔ Monitor Manager Internal Audit
Team

Steering Committee
- Auditor & Controller
- Purchasing Director

Advisory Board
- A/P
- Purchasing
- Internal Audit

System Admin
- Internal Audit

AX Users
- Core Depts
- User Depts
# Roles & Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Internal Audit</th>
<th>Core Depts</th>
<th>User Depts</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Administration</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication &amp; Coordination</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continuous Monitoring</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>End User Training</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Advisory Board</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>User Group</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Project Implementation

- **Specific Tasks Involved:**
  - Functional Requirements
  - Data Requirements
  - User Acceptance Testing

- **Throughout the Project:**
  - Monitor project status.
  - Resolve issues.
  - Communicate.
  - Get right people involved.
Deployment Plan

- Communication
  - Advisory Board Meetings
  - User Group Meetings
- Policies & Procedures Manual
  - System Navigation
  - Exception Resolution Procedures
- End User Training
- User Access Setup
Communication: Sample Slides
Why AX System?

Industry Best Practice...

COSO Internal Control framework

Monitoring Activities

- Conduct ongoing and separate evaluations
- Evaluate and communicate control deficiencies
Why AX System?

External Auditing Requirements...

- *Consideration of Fraud in a Financial Statement Audit* (AICPA SAS #99).

What does it Mean?

AX System...

• **Strengthen management controls** in business processes.

• Flag transactions inconsistent with County’s policies and procedures.

• Detect potential fraud, waste, and abuse.

• Enable management to identify, investigate, and resolve issues *before* they escalate.
AuditExchange
Screenshots
<table>
<thead>
<tr>
<th>Entity ID</th>
<th>Entity Name</th>
<th>Total Sum</th>
<th>Open Sum</th>
<th>Special Review</th>
<th>Returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCARD_CSG</td>
<td>PCARD_CSG</td>
<td>1008</td>
<td>1007</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>PCARD_DA</td>
<td>PCARD_DA</td>
<td>1178</td>
<td>1174</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>PCARD_DCSS</td>
<td>PCARD_DCSS</td>
<td>440</td>
<td>438</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>PCARD_DGS</td>
<td>PCARD_DGS</td>
<td>581</td>
<td>502</td>
<td>5</td>
<td>74</td>
</tr>
<tr>
<td>PCARD_DPW</td>
<td>PCARD_DPW</td>
<td>599</td>
<td>599</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PCARD_FG3</td>
<td>PCARD_FG3</td>
<td>21</td>
<td>16</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PCARD_HHSA</td>
<td>PCARD_HHSA</td>
<td>808</td>
<td>769</td>
<td>35</td>
<td>4</td>
</tr>
<tr>
<td>PCARD_LUEG</td>
<td>PCARD_LUEG</td>
<td>497</td>
<td>491</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>PCARD_OES</td>
<td>PCARD_OES</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>PCARD_PRK</td>
<td>PCARD_PRK</td>
<td>879</td>
<td>861</td>
<td>18</td>
<td>0</td>
</tr>
<tr>
<td>PCARD_PRO</td>
<td>PCARD_PRO</td>
<td>298</td>
<td>298</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PCARD_SHF</td>
<td>PCARD_SHF</td>
<td>1756</td>
<td>1754</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PTP_BLANK</td>
<td>PTP_BLANK</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PTP_COSD_AP</td>
<td>PTP_COSD_AP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PTP_COSD_FG3</td>
<td>PTP_COSD_FG3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PTP_CSG</td>
<td>PTP_CSG</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PTP_DA</td>
<td>PTP_DA</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PTP_DCSS</td>
<td>PTP_DCSS</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PTP_DGS</td>
<td>PTP_DGS</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PTP_DPW</td>
<td>PTP_DPW</td>
<td>11</td>
<td>11</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PTP_FG3</td>
<td>PTP_FG3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### Overview – Specific Entity

<table>
<thead>
<tr>
<th>Analytic:</th>
<th>Analytic Name:</th>
<th>Total Sum</th>
<th>Open</th>
</tr>
</thead>
<tbody>
<tr>
<td>AXEMA1-Invalid Cardholder</td>
<td>A1-Invalid Cardholder</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AXEMA10-Same Merchant/Amt/Dept</td>
<td>A10-Same Merchant/Amt/Dept</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>AXEMA14-Restricted Word</strong></td>
<td><strong>A14-Restricted Word</strong></td>
<td><strong>1007</strong></td>
<td><strong>1007</strong></td>
</tr>
<tr>
<td>AXEMA4-SOD Cardholder</td>
<td>A4-SOD Cardholder</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AXEMA5-SOD Verifier</td>
<td>A5-SOD Verifier</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AXEMA6-SOD Approver</td>
<td>A6-SOD Approver</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AXEMA7-SODApprover=Verifier/CH</td>
<td>A7-SODApprover=Verifier/CH</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### My Exceptions – Entity Summary

**Entity:** PCARD_CSG  
**From:** yyyy-mm-dd  
**To:** yyyy-mm-dd  
**State:** Open

<table>
<thead>
<tr>
<th>Entity ID</th>
<th>Entity Name</th>
<th>Total Sum</th>
<th>Open</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCARD_CSG</td>
<td>PCARD_CSG</td>
<td>1007</td>
<td>1007</td>
</tr>
</tbody>
</table>
### My Exceptions – by Analytic

#### AX Exception - My Exceptions

**Entity:** PCARD_CSG

**Analytic:** All

**From:** yyyy-mm-dd

**To:** yyyy-mm-dd

**State:** Open

### AX Exception

<table>
<thead>
<tr>
<th>Analytic:</th>
<th>Analytic Name:</th>
<th>Total Sum</th>
<th>Open</th>
</tr>
</thead>
<tbody>
<tr>
<td>AXEMA1-Invalid Cardholder</td>
<td>A1-Invalid Cardholder</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AXEMA10-Same Merchant/Am/Dept</td>
<td>A10-Same Merchant/Am/Dept</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>AXEMA14-Restricted Word</strong></td>
<td><strong>A14-Restricted Word</strong></td>
<td><strong>1007</strong></td>
<td><strong>1007</strong></td>
</tr>
<tr>
<td>AXEMA5-SOD Verifier</td>
<td>A5-SOD Verifier</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AXEMA6-SOD Approver</td>
<td>A6-SOD Approver</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AXEMA7-SODApprover=Verifier/CH</td>
<td>A7-SODApprover=Verifier/CH</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### Exception Details

<table>
<thead>
<tr>
<th>State ID</th>
<th>Analysis Date</th>
<th>Priority</th>
<th>Group</th>
<th>Super Department</th>
<th>Department</th>
<th>Division</th>
<th>Cardholder Name</th>
<th>Card Number</th>
<th>Cardholder Empl ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>2012-12-21 11:48:05</td>
<td>G5000</td>
<td>DS530</td>
<td>A7320</td>
<td>D7324</td>
<td></td>
<td><strong>AGUILAR, RICARDO</strong></td>
<td>**************1516</td>
<td>000000000000000000</td>
</tr>
<tr>
<td>Open</td>
<td>2012-12-21 11:48:05</td>
<td>G5000</td>
<td>DS530</td>
<td>A7320</td>
<td>D7322</td>
<td></td>
<td><strong>MULREAN, JAMES R</strong></td>
<td>**************0342</td>
<td>000000000000000000</td>
</tr>
<tr>
<td>Open</td>
<td>2012-12-21 11:48:05</td>
<td>G5000</td>
<td>DS520</td>
<td>A6190</td>
<td>D6192</td>
<td></td>
<td><strong>LEBDUSKA, CARYN</strong></td>
<td>**************1754</td>
<td>000000000000000000</td>
</tr>
</tbody>
</table>
Lessons Learned

The Ten Commandments

I. Thou shalt have no other gods before me
II. Thou shalt not make unto thee any graven image
III. Thou shalt not take the name of the LORD thy God in vain
IV. Remember the sabbath day to keep it holy
V. Honour thy father and thy mother
VI. Thou shalt not kill
VII. Thou shalt not commit adultery
VIII. Thou shalt not steal
IX. Thou shalt not bear false witness against thy neighbour
X. Thou shalt not covet
Ten Commandments

I. Thou shalt have no other analytics besides the high-impact ones.

II. Thou (auditor) shalt not make yourself a monitor.

III. Thou shalt not take thy data in vain, for the analytics will not forgive those who misuse the data.
Ten Commandments

IV. Remember the run day to keep it going.

V. Honor thy Steering Committee and Advisory Board, so that thy program may live long.

VI. Thou shalt not murder thy users, even when they complain.

VII. Thou shalt not mingle incompatible data.
Ten Commandments

VIII. Thou shalt steal ideas from user groups.

IX. Thou shalt not bear false positives to thy users ... where possible.

X. Thou (User Dept) shalt not covet thy neighbor’s analytic results ... thou have enough trouble of your own 😊.
Next Steps

• Maintain
  ◦ User Access Management
  ◦ Analytic Upkeep
  ◦ Upgrades

• User Training and Communication

• Strategy and Planning
  ◦ Stakeholder Feedback
  ◦ Design/Establish New Analytics
  ◦ Create Analytics for the Analytics
Thank You!
Contacts

Mady Cheng 858-495-5679
Mady.Cheng@sdcounty.ca.gov

Franco Lopez 858-505-6436
Franco.Lopez@sdcounty.ca.gov

Office of Audits & Advisory Services
County of San Diego