

CACS 2005 oceania
conference
Perth West Australia



*Information Systems
Audit and Control
Association®*

Continuous Monitoring A Strategy for more Effective Controls

John Hughes

IT Audit Systems Consultant

Continuous Controls Monitoring

- The need for continuous controls monitoring
- Conceptual model for continuous controls monitoring
- Types of controls that can be continuously monitored through technology
- Methodology for automated continuous controls monitoring
- Practical implementation issues

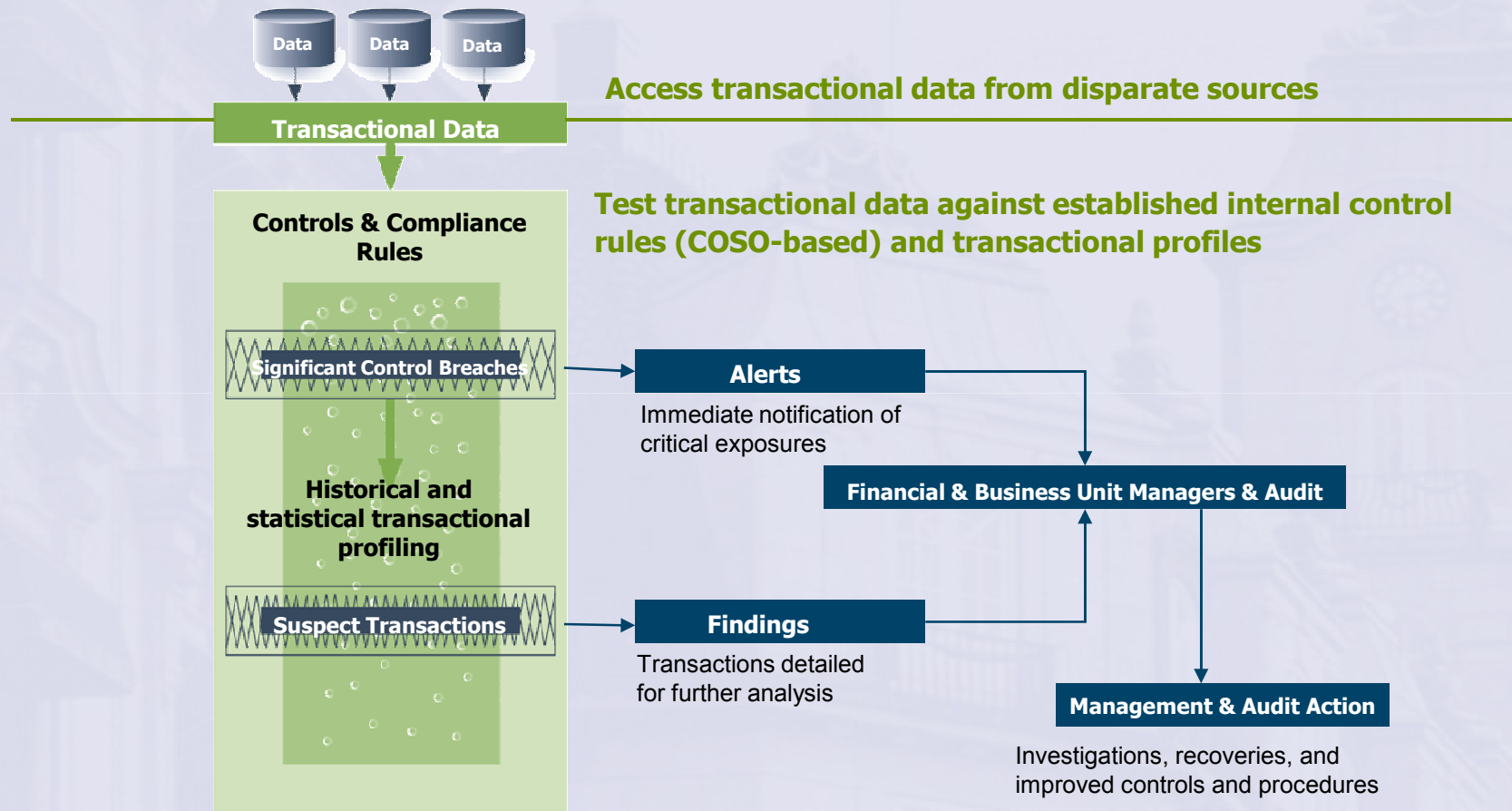
The Need for Continuous Controls Monitoring

- Continuous monitoring and auditing
 - Discussed for many years
 - Progress made – but limited
- Regulatory Compliance now driving the need
 - How to efficiently and cost effectively sustain controls assessment and testing efforts?
 - How to know on a timely basis when control deficiencies occur?
 - How to quantify the impact of control deficiencies?
 - How to improve effectiveness of controls
 - How to gain assurance over effectiveness of controls

Model for Continuous Monitoring of Controls

- Identify the control rule for each internal control point (using COSO framework)
- Establish tests that, using transactional data analysis, will validate each control rule
- Establish tests that will identify suspect transactions, using transactional profiling techniques
- Subject all transactions to a suite of tests on a regular, timely basis
- Identify all transactions that fail the tests
- Notify the appropriate personnel
- Investigate any transactions that fail and, as appropriate,
 - Correct the transactions
 - Correct the control problem

Continuous Monitoring Model



The Result

- Timely determination whether controls in application and financial reporting systems are operating effectively
- Rapid identification of specific deficiencies and anomalies
- Independent assurance of integrity of transactions processed by business application systems
- An additional layer of control
- Reduction in costs and revenue leakage
- Improved efficiency and effectiveness of regulatory assessments
- Quantification of control deficiencies

Continuous Controls Monitoring: Management is Responsible

MANAGEMENT'S RESPONSIBILITY

**To implement and maintain
effective controls**

AUDITORS' RESPONSIBILITY

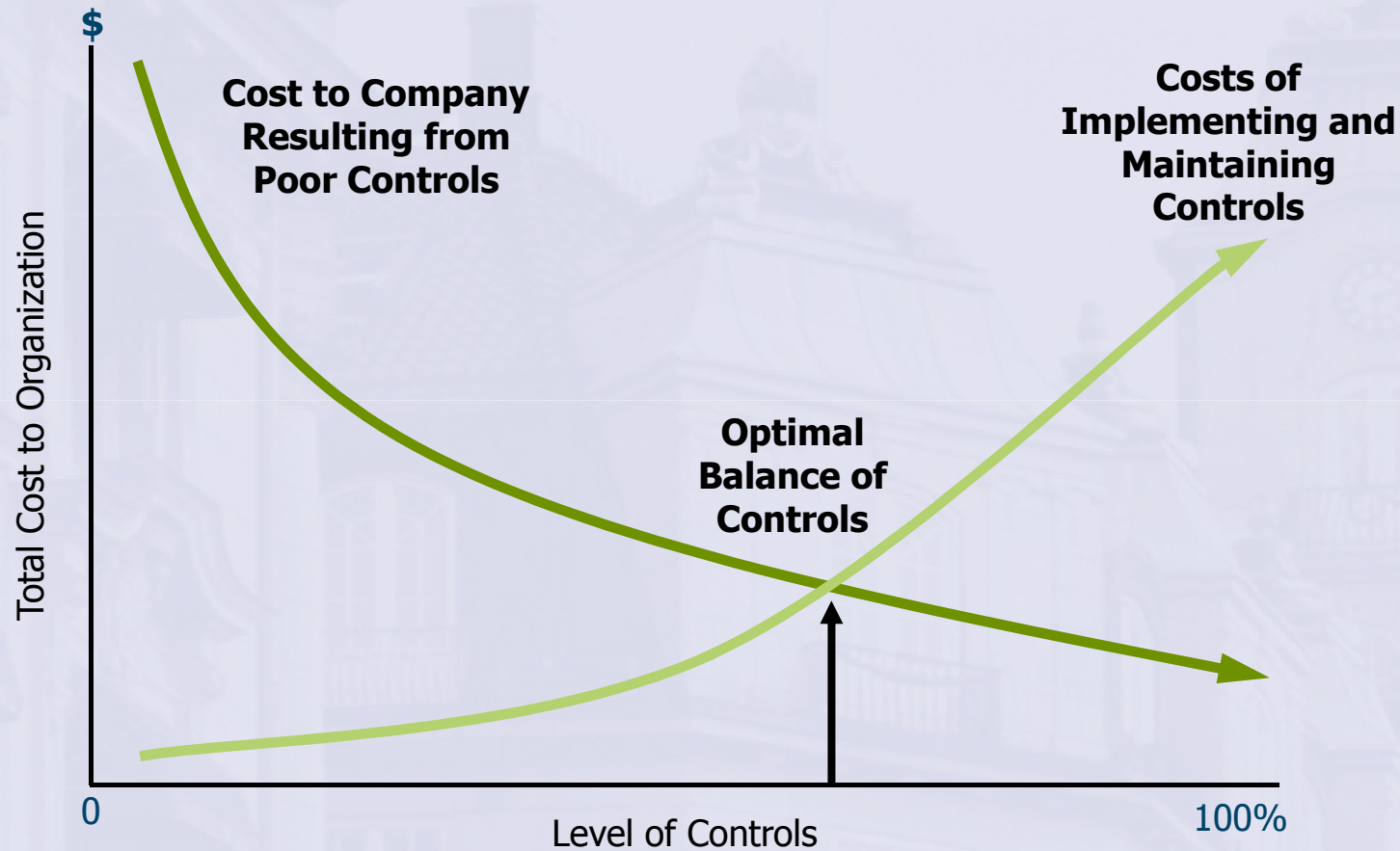
**To ensure management has
fulfilled responsibility**

Controls Infrastructure

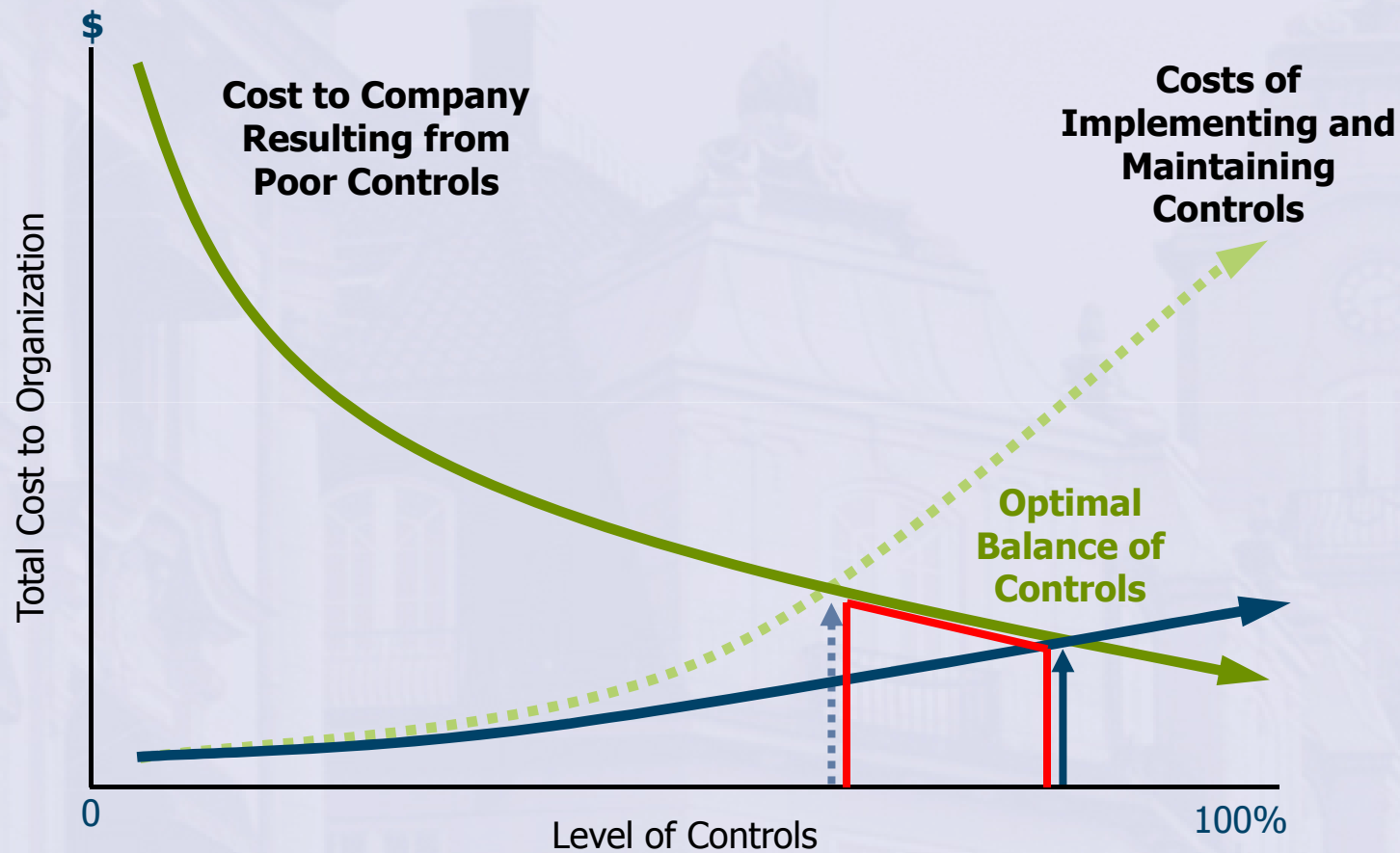
**Continuous Controls Monitoring
Framework**

Management and audit are both stakeholders in
Continuous Controls Monitoring.

Cost/Benefits of Controls



ROI for Continuous Controls Monitoring



Automation of Controls Testing

What types of controls and deficiencies can be tested through automated continuous monitoring?

- Any control or breakdown that can be evidenced through computerized data e.g.:
 - Business process financial controls
 - Segregation of Duties
 - I.S. security controls
 - Application control settings / ERP configuration

Functional Requirements of a Continuous Controls Monitoring Framework

- Able to access and normalise disparate data from across the enterprise
- Offer comprehensive range of tests to effectively address control points
- Provide timely testing of data and reporting of results
- Handle large transactional volumes with no negative impact on operational system performance
- Provide variable parameters for tests
- Manage alert notifications
- Security
- Ability to view and manage results

Implementation Challenges

- Timely data access
- Minimizing impact on systems' operational performance
- Defining appropriate analytics
- Setting appropriate thresholds for exceptions
- Developing suitable scoring / weighting mechanism to prioritise exceptions
- Management of results

Automation of Controls Testing

- Must be possible to define rule of a control, e.g.:
 - invoice payment should not be entered and approved by same person
 - payments >\$X must be approved by Y
 - inventory items shipped must be matched by invoice details
 - ERP application control for duplicate payments should be set on
- Or, indicators of control breaches need to be able to be established, e.g.:
 - Transactions that fall outside of statistical norms
 - Profile/trend analysis

Methodology for Continuous Controls Monitoring



- Define High Level Overview
 - Business process flow chart outlines entire business cycle
 - Key activities are identified for each business process

Methodology for Continuous Controls Monitoring



- Identify key risks and control objectives for each activity
 - Accuracy
 - Authorization
 - Completeness
 - Validity
 - Efficiency and Effectiveness
 - Segregation of Duties
 - Regulatory Compliance

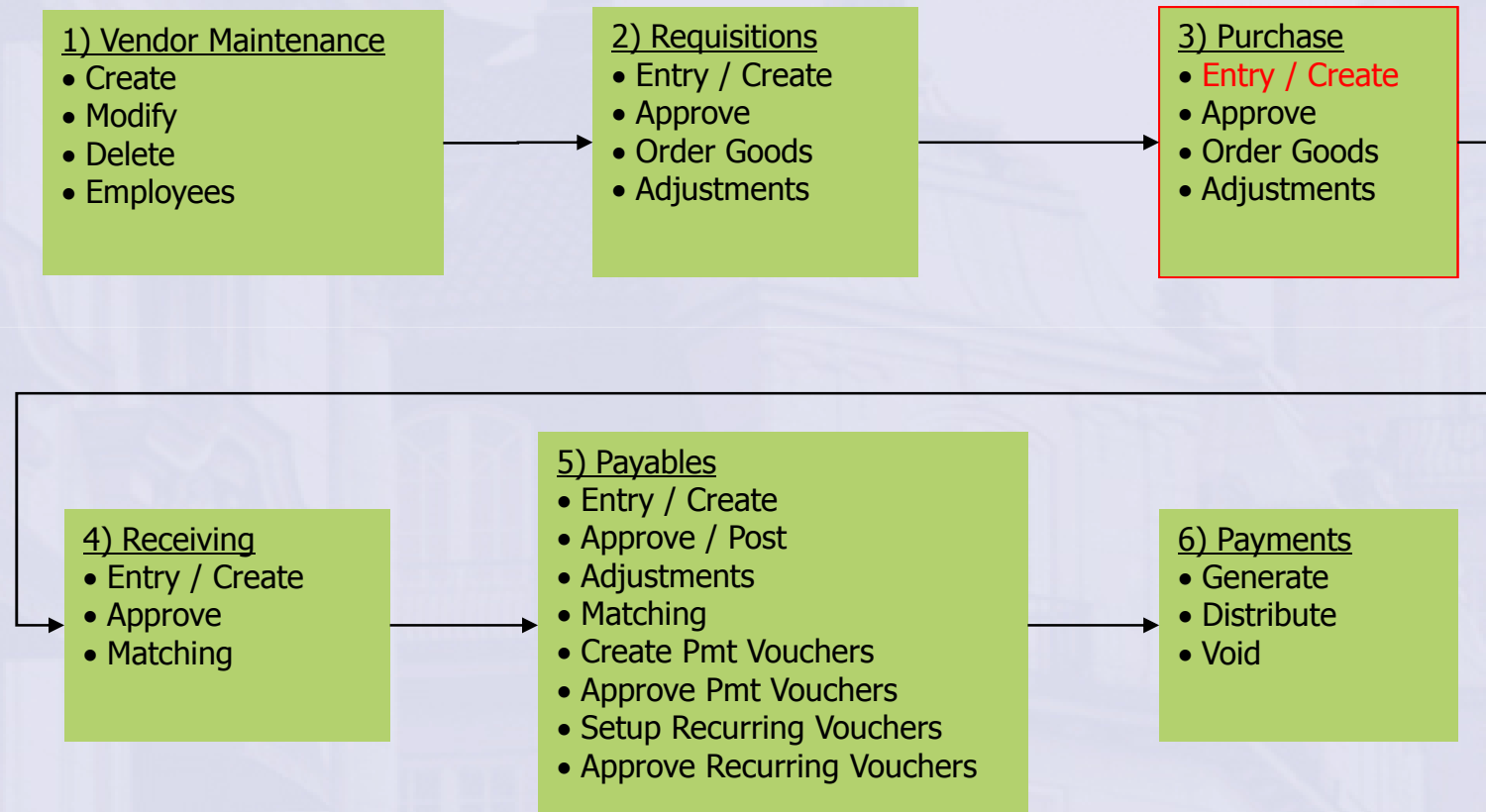
Methodology for Continuous Controls Monitoring



- Control objectives translated into test analytic objectives
- Test details designed and developed into specific analytics

Define Business Process Overview

Purchase-to-Payment Cycle: Activities



Define Control Objectives

- Purchase**
- **Entry / Create**
 - Approve
 - Order Goods
 - Adjustments

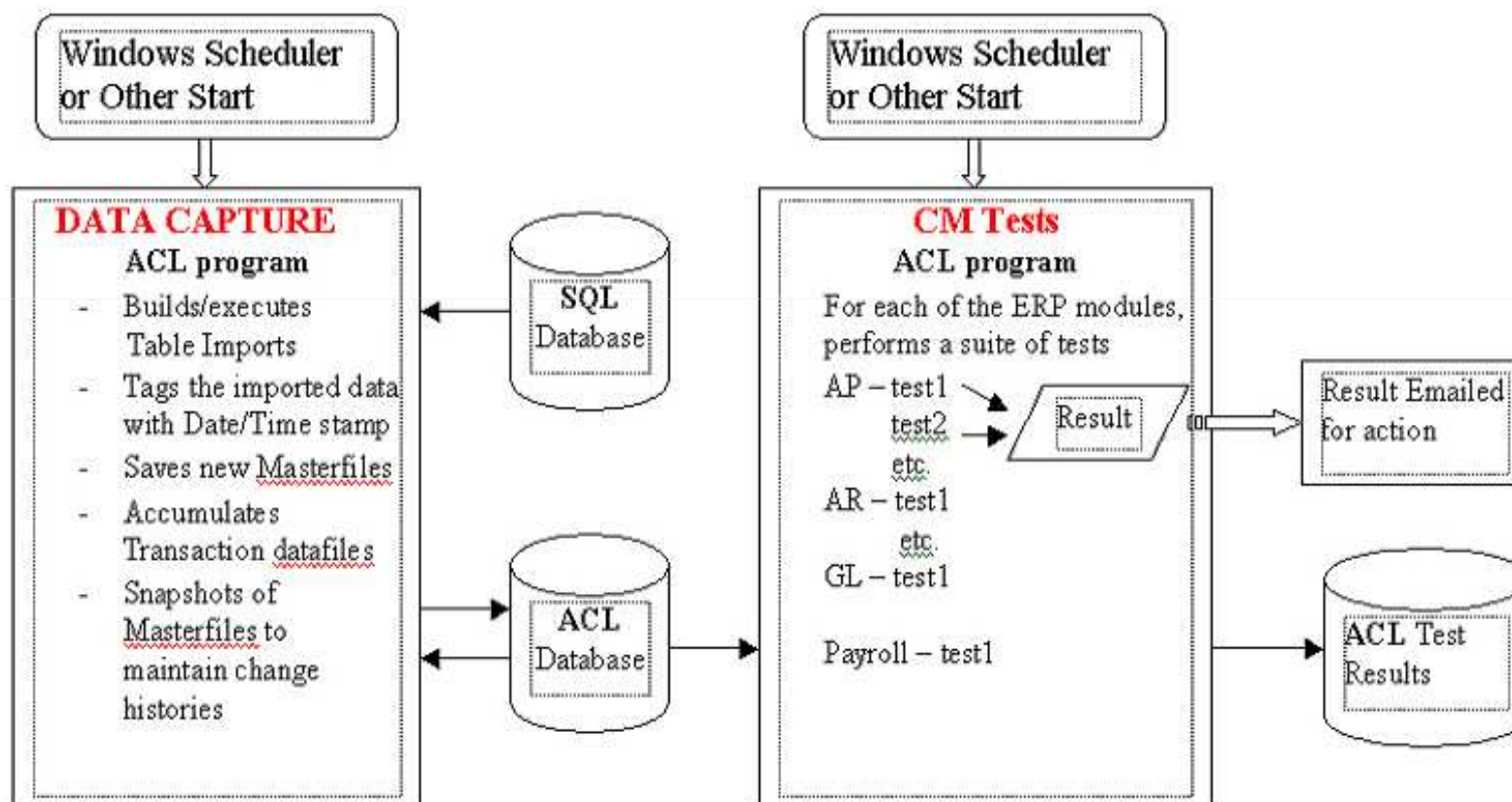
Activity	Control Objective	Assertion
Create Purchase Order	To ensure all critical data is captured.	Completeness
	To ensure all data entered is valid.	Validity
	To ensure that only approved PO's are issued.	Authorization
	To ensure PO's are only entered once.	Accuracy
	To ensure that PO's are within approved employee purchasing limits	Authorization
	To ensure no purchases are made from companies or individuals listed on OFAC terrorist lists	Regulatory

Perform Risk / Impact Ranking

- Purchase**
- **Entry / Create**
 - Approve
 - Order Goods
 - Adjustments

Activity	Control Objective	Transactional	Control Risk Ranking	Business Impact	Overall (e*f)
Create Purchase Order	To ensure all critical data is captured.	N			0
	To ensure all data entered is valid.	Y	3	3	9
	To ensure that only approved purchases are issued.	Y	3	3	9
	To ensure PO's are only entered once.	Y	2	3	6
	To ensure that PO's are within approved employee purchasing limits	Y	2	3	6
	To ensure no purchases are made from companies or individuals listed on OFAC terrorist lists	Y	3	3	9

Overview – example Continuous Monitoring model



Example of Accounts Payable Test Summary - Click on AP_TestName to drill through

CCM_Demonstration.ACL - ACL Version 8

File Edit Data Analyze Sampling Applications Tools Server Window Help

Project Navigator

- CCM_Demonstration.ACL
 - Data
 - GP_Companies
 - HQTRS
 - KELEC
 - TEST
 - TEST_AP_Import
 - TEST_AP_MasterFiles
 - TEST_AP_TestResults
 - AP_Test_Transactions**
 - TEST_AR_Import
 - TEST_AR_MasterFiles
 - TEST_AR_TestResults
 - TEST_GL_Import
 - TEST_GL_MasterFiles
 - TEST_GL_TestResults
 - Parameters
 - Scripts
 - _AutoStart
 - _UserStart
 - Admin
 - Import
 - ModTests
 - Subroutines
 - CCM_Demonstration
 - Log_050905_133738_Auto
 - Log_050905_133940_Auto

AP_Test_Transactions **Classify**

As of: 20050915 13:56:11

Command: CLASSIFY ON AP_TestName SUBTOTAL SUBTOTAL TO SCREEN

Table: AP_Test_Transactions

AP_TestName	Count	Percent of Count	Percent of Field	SUBTOTAL
<u>PO Passed all Tests</u>	8,788	86.72%	87.82%	54,908,082.37000
<u>Modified Purchase Order</u>	40	0.39%	0.47%	293,048.42000
<u>Purchase Order vs Invoice Pricing</u>	371	3.66%	2.97%	1,858,962.64000
<u>Same Creator and Authoriser for PO</u>	333	3.29%	2.19%	1,368,948.58000
<u>Split Purchase Order</u>	133	1.31%	1.21%	754,531.20000
<u>Stale Purchase Order</u>	450	4.44%	5.13%	3,208,813.28000
<u>Unauthorised Purchase Order</u>	19	0.19%	0.21%	131,187.21000
Totals	10,134	100%	100%	62,523,573.70000

Example of a Drill Through to a Test Record Subset

CCM_Demonstration.ACL - ACL Version 8

File Edit Data Analyze Sampling Applications Tools Server Window Help

AP_Test_Transactions Classify

Filter: [AP_TestName = "Same Creator and Authoriser for PO "] Index: (None)

	AP_TestName	PONUMBER	ATUS	TGRP	YPE	USER2ENT	CONFIRM1	DOCDATE	LSTEDTDT	LSTPRT
9200	Same Creator and Authoriser for PO	0029880	2	1	1	sreeve	shannon reeve	20050406	20050406	200504
9201	Same Creator and Authoriser for PO	0029966	2	1	1	sreeve	shannon reeve	20050406	20050406	200504
9202	Same Creator and Authoriser for PO	0030119	2	1	1	sreeve	shannon reeve	20050405	20050405	200504
9203	Same Creator and Authoriser for PO	0030934	2	1	1	bmathison	Briony	20050317	20050317	200504
9204	Same Creator and Authoriser for PO	0030945	2	1	1	sreeve	Shannon Reeve	20050316	20050318	200504
9205	Same Creator and Authoriser for PO	0030947	2	1	1	bmathison	Briony	20050317	20050317	200504
9206	Same Creator and Authoriser for PO	0030962	2	1	1	bmathison	Briony	20050317	20050317	200504
9207	Same Creator and Authoriser for PO	0030965	2	1	1	sreeve	Shannon Reeve	20050316	20050318	200504
9208	Same Creator and Authoriser for PO	0030968	2	1	1	sreeve	Shannon Reeve	20050316	20050318	200504
9209	Same Creator and Authoriser for PO	0030971	2	1	1	sreeve	SHannon Reeve	20050316	20050318	200504
9210	Same Creator and Authoriser for PO	0030972	2	1	1	sreeve	Shannon Reeve	20050316	20050318	200504
9211	Same Creator and Authoriser for PO	0030989	2	1	1	bmathison	Briony	20050317	20050317	200504
9212	Same Creator and Authoriser for PO	0030991	2	1	1	bmathison	Briony	20050317	20050317	200504
9213	Same Creator and Authoriser for PO	0031002	2	1	1	bmathison	Briony	20050317	20050317	200504
9214	Same Creator and Authoriser for PO	0031008	2	1	1	bmathison	Briony	20050317	20050317	200504
9215	Same Creator and Authoriser for PO	0031009	2	1	1	bmathison	Briony	20050317	20050317	200504
9216	Same Creator and Authoriser for PO	0031017	2	1	1	bmathison	Briony	20050318	20050318	200504
9217	Same Creator and Authoriser for PO	0031032	2	1	1	sreeve	Shannon Reeve	20050318	20050318	200504
9218	Same Creator and Authoriser for PO	0031041	2	1	1	bmathison	Briony	20050318	20050318	200504
9219	Same Creator and Authoriser for PO	0031048	2	1	1	bmathison	Briony	20050318	20050318	200504
9220	Same Creator and Authoriser for PO	0031091	2	1	1	sreeve	Shannon Reeve	20050321	20050321	200504
9221	Same Creator and Authoriser for PO	0031096	2	1	1	bmathison	Briony	20050321	20050321	200504
9222	Same Creator and Authoriser for PO	0031101	2	1	1	sreeve	Shannon Reeve	20050321	20050321	200504
9223	Same Creator and Authoriser for PO	0031112	2	1	1	sreeve	Shannon Reeve	20050321	20050414	200504
9224	Same Creator and Authoriser for PO	0031113	2	1	1	sreeve	Shannon Reeve	20050321	20050414	200504
9225	Same Creator and Authoriser for PO	0031130	2	1	1	bmathison	Briony	20050322	20050407	200504
9226	Same Creator and Authoriser for PO	0031131	2	1	1	sreeve	Shannon Reeve	20050322	20050322	200504
9227	Same Creator and Authoriser for PO	0031136	2	1	1	sreeve	Shannon Reeve	20050322	20050418	200504
9228	Same Creator and Authoriser for PO	0031146	2	1	1	sreeve	SHANNON REEVE	20050322	20050415	200504
9229	Same Creator and Authoriser for PO	0031176	2	1	1	sreeve	Shannon Reeve	20050323	20050407	200504
9230	Same Creator and Authoriser for PO	0031195	2	1	1	sreeve	Shannon Reeve	20050323	20050414	200504
9231	Same Creator and Authoriser for PO	0031196	2	1	1	sreeve	Shannon Reeve	20050323	20050415	200504
9232	Same Creator and Authoriser for PO	0031198	2	1	1	sreeve	Shannon Reeve	20050323	20050415	200504
9233	Same Creator and Authoriser for PO	0031206	2	1	1	sreeve	Shannon Reeve	20050323	20050415	200504

Default_View

AP_Test_Transactions ?/10,134 Global Filter: (AP_TestName = "Same Creator and Authoriser for PO ")

Compliance Requirements

- Compliance readiness & sustainability
- Reduced time for reporting/signoff
- Streamlined external audit review

Continuous Controls Monitoring

Business Performance Optimization

- Revenue maximization
- Operational efficiencies
- Profit maximization
- Fraud reduction

Good Governance is Good Business

For More Information:

John Hughes

ACL Consultant

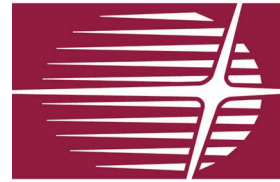
jhughes@magsys.com.au

www.magsys.com.au

Mob: 0412 200372

Tel: (02) 4869 5098

CACS 2005 oceania
conference
Perth West Australia



*Information Systems
Audit and Control
Association[®]*

Thank you!